Perceptions of online fraud and the impact on the countermeasures for the control of online fraud in Saudi Arabian financial institutions

A thesis submitted for the degree of Doctor of Philosophy

By

FAISAL ALANEZI

2015

College of Engineering Design and Physical Sciences

Department of Computer Science

Brunel University

ABSTRACT

This study addresses the impact of countermeasures in the control and prevention of online fraud in Saudi Arabia and the influence of the environmental context. Combatting online fraud is facilitated when the public is fully educated and is aware of its types and of the prevention methods available. People are reliant on the Internet; the possibility of being breached by hackers and fraudsters is growing, especially as socialising, online shopping and banking are carried out through personal computers or mobile devices. Online fraud has been described as an epidemic that has spread to most online activities. Its prevalence has been noted to be in regions where there is high adoption of e-commerce, and, along with it, large online financial transactions. The argument is therefore the measures taken are either are inadequate or have failed to effectively address all the issues because of the organisational and environmental context of the country. This research aims to examine online fraud perceptions and the countermeasures designed and used by financial institutions in Saudi Arabia to control and prevent online fraud in its environmental context, to examine the effectiveness/impact of the countermeasures and to examine the factors that may affect/influence the impact of the countermeasures. The qualitative method approach was chosen to ensure balanced coverage of the subject matter. The nature of the research requires a broader, in-depth, examination of the experiences of the participants from their own perspective. Meanwhile levels of awareness are low, because of lack of knowledge and training, a lack of government sensitisation and the religious inclinations of the population. The findings also confirm the efforts of organisations to put in place countermeasures using various technological means, coupled with procedural controls and checks. The measures create obstacles to most customers, who find it cumbersome to engage in online activities because of those procedures and checks. The findings also show two types of regulations: government and organisational rules, with different foci and purposes, which are mostly centred on the monitoring of Internet operations and operational guidelines. The enforcement of rules in the light of prosecuting offenders has also been minimal and passive. The countermeasures of most banks/organisations mostly focus on prevention and detection. However, the findings suggest that the activities in each component and their interrelationships have a collective impact on combatting online fraud. The success of any effort or approach to combat fraudulent activities therefore depends on the activities of the four countermeasure components.

ACKNOWLEDGEMENTS

This work is dedicated to my father Mr Yousif Alanezi, who has given great support and encouragement throughout my study, whilst I was living in the UK, without whom, I would never have achieved this work. It is also an opportunity for me to extend my thanks to the Minister of Higher Education in Saudi Arabia for giving me the opportunity to commence my study in the UK. I sincerely thank my supervisor Dr Laurence Brooks for his help, guidance and patience. To my friends and my family, special thanks for their continued support.

Table of Contents

Lists of Tables

List of Figures

CHAPTER 1

INTRODUCTION

The world has since the 1990s experienced great technological innovations that have revolutionised the business and social world (Bartling, & Friesike, 2014). The business world has become more reliant on technological breakthroughs as business processes and transactions are now mainly technologically driven. The Internet revolution, which is an outcome of information technology breakthrough, has now become the bedrock for business revolution (Fettweis, & Alamouti, 2014). The commercialisation of the worldwide web has seen the rapid growth of web-based transactions, which have created various new opportunities. Many businesses have explored these online opportunities to provide better and easier services to their customers and gain competitive advantage. This aspect of the online transaction is popularly referred to as electronic commerce.

E- Commerce is increasing rapidly and creating new opportunities for merchants, but at the same time creating opportunities for fraudulent practices. Criminals have tried in many ways to take advantage of the new opportunities to carry out online fraud against both the sellers and buyers. Common cyber-based criminal activities such as online fraud and phishing attacks are now perpetrated through the use of false identity, fraudulent and counterfeited documents as a result of the increasing reliant on online transactions

(Raj, 2015).

Electronic commerce therefore presents potential problems for online users both personal and business use (Stringham, 2005). The ever-expanding connections enabled by the Internet are also seen to attract the possibility of significant losses through online fraud, which could be a major threat to electronic commerce (Coyne, 2005). Fraud on the Internet, which is 20 times higher than offline fraud, is thus developing into a major issue for consumers, businesses, and governments (Snyder, 2000; Bajari and Hortaçsu, 2004; Waters, 2003).

It is described as a huge and rapidly growing epidemic that has spread through most online activities such as electronic banking, online auctions, e-marketing etc, (Waters, 2003). Online fraud is thus generally described as the use of online facilities to carry out dubious business transactions with the intention of deceiving or defrauding persons, organisations or governments (Albert, 2002). Its prevalence has been noted to be in regions where there is high adoption of e-commerce and with large online financial transactions.

The high rate of Internet acceptance and penetration in the Gulf region has revolutionised business transactions and the economies of the nations in the region, but has also seen the rise of online fraud in the region with millions of dollars lost to fraudulent practices (Joseph & Lunt, 2006; Salazar & Low, 2011; Deloitte, 2011).

Saudi Arabia is arguably one of the wealthiest countries in the Middle Eastern region. It has the highest number of Internet users supported by government policies and the use of advanced technologies in most areas of governance

and commerce, with a 62.97% penetration level and subsequently is vulnerable to online fraud (Karake, Shalhoub and Al Qasimi, 2003).

The region and the world in general have experienced the increasing virtual attack on virtual wallets and online accounts of citizens (Brytting, Minogue & Morino, 2011). Online fraudsters have therefore perpetrated their fraudulent practices in online banking, auction trading, and e-commerce, to earn dubious money, while preying on careless online users or employees of organisations (Deloitte, 2011; Hawkins, Yen and Chou, 2000). The increase in online fraud is reflected in the reported number of losses and the complaints made by victims to banks and other law enforcement agencies (ICCC, 2008; National Authority report, 2012).

This increasing number of reported online fraud losses, complaints and the negative impact of online fraud on businesses and global economies thus make online fraud a worldwide challenge (Coyne, 2005; Montague, 2011). Governments and organisations have made different efforts in different areas such as regulations, monitoring organisations, users, and the use of modern technology to control the rate of online fraud. The different measures put in place have however yielded little or no success, as the rate of online fraud still remains high in most countries and regions. The argument may therefore be that the measures taken are either not comprehensive enough, inadequate or have failed to effectively address all the issues of online fraud due to the organisational and environmental context of Saudi Arabia.

This research is therefore aimed at examining the impact of the countermeasures put in place by financial institutions in Saudi Arabia to control

and prevent online fraud in their environmental context. This is with the view of determining the factors and issues influencing the countermeasures, and the development of a framework that would facilitate effective control of online fraud in Saudi Arabia.

The study was conducted to determine the impact of countermeasures in the control and prevention of online fraud in Saudi Arabia and the influence of the environmental context.

1.1 Background Research

A general description of fraud is that it is a set of deceptive activities engaged by a partner in a business relationship for personal gains and therefore an intentional act to deceive through false information, claim or the suppression of the truth (Albert, 2002). The penetration of the Internet in economies and commerce and the changes it has brought in the way business transactions are done have opened up avenues to perpetrate Internet fraud. Electronic commerce has had a rapid increase generating total online transactions of about 1.5 trillion dollars globally in 2014 from about 268 billion dollars in 2008 (Criteo, 2015; Javelin Strategy & Research, 2008).

The Internet has thus enabled the creation of a global electronic market place offering the opportunities for merchants around the globe to engage in commerce with anyone in any place. Business transactions including invoicing, payments and goods deliveries are done online mostly in non-face-to-face transactions where only the documentations submitted online are relied upon. Montague (2011) stated that fraud in e-commerce channels is very common

and has become so integral in the conducting of business that it now has become a major challenge.

The impact of electronic commerce expansion may therefore have created new channels for online fraud, thus exposing customers of electronic commerce to potential frauds (Stringham, 2005; Coyne, 2005), which may increasingly become complicated to prevent (Montague, 2011).

The ability to transact online business through online documentations and verbal instructions may also have exposed online users to fraudulent solicitations and transactions with the use of false documentation or identity theft. Electronic commerce platforms have therefore created opportunities for Consumer-present fraud (CP) and consumer-not-present fraud (CNP). CNP fraud usually involves transactions carried out between two or more parties where the customer's presence is not physical but represented by instructions through an online medium, which makes the use of false documentation or identity theft easily committed.

Online transactions are normally carried out in three major different ways namely (i) phone-in orders (telephone order); (ii) catalogue orders (mail order); and (iii) e-commerce orders, which are all online based (Montague, 2010).

Online fraud is therefore perpetrated using any component of the Internet for fraudulent solicitations and transactions (Albert, 2002) in different disguises, forms or shades. Common forms include online identity theft fraud, online retail schemes and online auction fraud. The negative impact of online fraud in global commerce in the last decade has attracted attention from organisations and

governments demanding for ways to minimise its negative impact (Moore, 2010). There have been calls for an examination of security measures and countermeasures adopted by organisations to be focused on the challenges of online fraud in global commerce and particularly in the gulf region which has seen the devastating impact of traditionalism and conservatism on the countermeasures on online fraud (Arab Region Internet and Telecom, 2001).

Online fraud has reached epidemic proportions in global business and in particular in the Gulf Cooperation Council because of the growth of user base (GCC) (Salazar & Low, 2011; El-Guindy, 2008), i.e. an economic cooperation organisation established in 1981 to bring together countries namely: Saudi Arabia, Kuwait, Bahrain, Oman, United Arab Emirates and Qatar that have different levels of economic development but the same language, culture and religion. Online users in the GCC are increasing significantly as a result of various online services being introduced into the economy by the governments. It is reported that large amounts of financial transactions flow through the economies of the GCC region, which also has a very high rate of economic development and technological advancement. The adoption of the Internet and e-commerce transactions in large quantities may have attracted and given rise to online fraudulent activities but the huge proportion of the online fraud and its continual growth may be attributed to other factors. The lack of legal regulation, such as security protection, privacy protection, may also have had some impact on the rise of online fraud in some regions.

Online fraud has therefore become an issue of concern and a major challenge to organisations and governments globally, particularly in the Gulf Corporation Council (GCC), where a large number of financial transactions have occurred

online, further increased by the high acceptance and penetration of the internet technology in the region (Stringham, 2005; El-Guindy, 2008). The Gulf area of the Middle East has a very high rate of Internet penetration and a very high rate of economic development and technological advancement, which has encouraged a large number of financial transactions to flow through the economies of the GCC region. Its been reported that 14% of organisations in the GCC region have lost more than 20 million US dollars on account of fraudulent online activities, while 7% of individual users lost more than 10 million US dollars (Joseph & Lunt, 2006; Salazar & Low, 2011; Deloitte, 2011). However, the table below illustrates the top 20 countries with a high risk of online attack and Saudi Arabia occupies the 16th position (Kaspersky, 2014).

Rank	Country	% Of users
1	Russia	53.81%
2	Kazakhstan	53.04%
3	Azerbaijan	49.64%
4	Vietnam	49.13%
5	Armenia	48.66%
6	Ukraine	46.70%
7	Mongolia	45.18%
8	Belarus	43.81%
9	Moldova	42.42%
10	Kyrgyzstan	40.06%
11	Germany	39.56%
12	Algeria	39.05%
13	Qatar	38.77%
14	Tajikistan	38.49%
15	Georgia	37.67%
16	Saudi Arabia	36.01%
17	Austria	35.58%
18	Lithonia	35.44%
19	Sri Lanka	35.42%
20	Turkey	35.40%

Table 1 Top 20 countries encountering High-risk online resource (Kaspersky security bulletin, 2014).

This seriousness of online fraud worldwide has made the issue of control and prevention a major challenge globally (Coyne, 2005; Montague, 2011). Governments and organisations have made various efforts in different areas, encompassing regulations, the monitoring of organisations, users and the use of modern technology to control the rate of online fraud. The different measures put in place have, however, yielded little or no success, as the rate of online fraud remains high in most countries and regions. The argument may therefore be that the measures taken are either not comprehensive enough, inadequate or have failed to address effectively all the issues of online fraud, as a result of the organisational and environmental context of the country.

This research aims therefore to examine the impact of the countermeasures put in place by financial institutions in Saudi Arabia to control and prevent online fraud in an environmental context. This is with the view of determining the factors and issues influencing the countermeasures, and the development of a framework that would facilitate effective control of online fraud in Saudi Arabia.

1.2 Problem Statement

By the contrast to the previous definition, fraud is a part of deception, and is the consequence of some misrepresentation that has been intentionally levelled at the victim by another individual (Albrecht *et al*., 2009). In the context of E-commerce the unlawful miss-match of information between two parties, subsequent in one-sided and illegal online business (Xiao & Benbasat, 2011).

The wide acceptance of electronic commerce has also introduced various channels of payments and electronic payments that may have also created avenues or platform to perpetrate fraudulent practices. The ever-expanding connections enabled by the Internet are also seen to attract the possibility of significant losses through online fraud that could be a major threat to electronic commerce (Coyne, 2005).

Other factors that may be responsible for the growth of online fraud particularly in the gulf region and the countermeasures adopted by organisations to fight online fraud are discussed in the following sections below.

1.3 Factors Responsible for Online Crime in the GCC Region

The factors identified to have affected the growth of online fraud and other cyber-crime in Saudi Arabia and other countries in the Gulf region include, among others, growth in the user base, poor security awareness, lack of training in law enforcement and lack of regulation (El-Guindy, 2008).

1.3.1 Increase in User Base

It is argued that the number of online users in the Gulf region is increasing, and may rise above the number of users in the rest of the world, which also increases the level of potential online abuse in the region. For example the acceptance of the culture of e-commerce and the influence of globalisation and technological innovations has contributed to the increase in the user base in Saudi Arabia. The government's intervention in the provision of Internet connections and a technology base for the economy has also contributed to the expansion of the online user base. The number of Internet users grew from

about 200,000 in 2000 to about 18 million in 2014 (BCG, 2012: internet world stats, 2014). (See Table below).

The average Internet economy growth rate of Saudi Arabia is 19.5 percent, which is relatively high compared to other countries in the gulf region and developed countries such as Russia with 18.3% (Munir Al-Sari, 2011).

Year	Users	Population	% Population
2000	200 000	21, 624 ,422	0.9%
2003	1 500 000	21, 771, 609	6.9%
2005	2 540 000	23, 595, 634	10.8%
2007	4 700 000	24, 069, 943	19.5%
2010	9 800 000	25, 731, 776	38.1%
2012	13,000,000	26,534,504	49.0
2014	18,300,00	27,752,316	61.24%

Table 2 Growth of Internet users in Saudi Arabia resource (http://www.internetworldstats.com/stats5.htm).

The introduction of Internet-based electronic finance offers various great opportunities for banks to expand their client base and revolutionise their business operations. The adoption of electronic banking has also encouraged many users to accept online use of banking transactions. Online banking, although mainly set up to provide useful information to customers in Saudi Arabia, also allows customers to carry out various financial transactions through the internet from their PCs and smart phone at home or anywhere. Some Saudi banks, such as the Saudi Investment Bank and the Saudi

American Bank, have also implemented provision of full Internet banking services (Jasimuddin, 2001). The increasing number of online users has also increased the number of business transactions and the volume of financial exchanges carried out online, which may have been a big attraction to online fraudsters.

1.3.2 Lack of Security Awareness

The growth of the Internet and e-commerce has also been noted to be accompanied by the concern for privacy and the security of users' information online (Miyazaki and Fernandez, 2000). The effective and efficient use of e-commerce may therefore depend on having adequate privacy and security arrangements for users' information. All the parties in online transactions, the consumers and the organisations may have roles to play in the security of information. Lack of security awareness or ineffectiveness of security awareness programs among users, both public and private, have raised concerns about the growth in online fraud in the Gulf region. The Ministry of Trade and Industry in Riyadh, Saudi Arabia attributed the increase of Internet and online fraud to lack of awareness and knowledge of E-commerce and inadequate knowledge of information technology security in offices.

1.3.3 Regulation

The lack of special regulation and effective enforcement agencies in the region may have contributed to the high rate of online fraud in the region. The Saudi Arabian government responded by introducing a variety of measures, including criminal sanctions against trespassers, but they have so far not been effective. Even the adoption of religious legislative instruments, such as *Sharia Law*, has

not done much to resolve the crisis in online fraud (Smith, 2001; Algamdi et el, 2012).

1.3.4 Technological Infrastructures

Online fraud can be defined as fraud perpetrated using the technological innovations that made online business popular. The detection of online fraud using technological infrastructures has thus become an important issue for exploration (Yufeng Kou *et al.*, 2004). Another problem facing government agencies and law enforcement bodies in the GCC is the lack of a technology and specialists that make reports on online fraud cases to law enforcement agencies; that causes an increasing burden and detection difficulties for fraud prevention at an effective level (Salazar & Low, 2011).

1.4 Countermeasures

In response to the threats of online fraud particularly in the Gulf region, organisations and governments have developed a variety of measures, including criminal sanctions against trespassers, which have not been effective, due to a lack of awareness in terms of online security among law enforcement agencies (Elnaim, 2013). The representatives of those agencies sometimes simply do not understand the difference between simple online transactions and hacking, thereby providing grounds for increasing fraud. This lack of awareness and confusion by the law enforcement agencies could be attributed to the primary problem of the definition and analysis of cyber-crime, on account of the absence of a consistent current definition, even among the law enforcement agencies that have responsibility for combatting online fraud.

There is therefore no specific referent in law to guide any one particular organisation to design countermeasures (Majed, 2008).

Even the adoption of legislative instruments such as Sharia Law does not contribute much to the resolution of the problem (Ballantyne, 1986). Saudi Arabia is a very religious conscious state and the legal system is mostly based on the sharia law and other religious customs however lack of necessary input from religious leaders and lack of awareness makes them volatile to the issues of online fraud prevention and detection. Another problem faced by government agencies and law enforcement bodies in the Gulf region is the lack of technology and specialists to effectively detect or prevent online fraud (Salazar & Low, 2011). Moreover, even if the crime is reported to law enforcement bodies, online fraud cannot be dealt with effectively on account of the increasing number of incidents overwhelming the agencies.

In the private sector, no effective measures, apart from technological, can be undertaken, because the private sector has no feasible influence on law enforcement bodies, apart from bringing actions in courts (Montague, 2010). Therefore, the private sector has fewer chances to combat cyber-crimes or online fraud than public authorities do. Following the example of Western counterparts, the private sector can create and assign special teams, which can react upon discovery of such cases of online fraud and crime. Thus, for instance, the establishment of a team could be proposed to serve the function of emergency response (Hawkins *et al*., 2000). It could coordinate responses from member teams when large-scale incidents of fraud take place. There is

also the need to investigate the causes of security breaches in order to understand the vulnerabilities of system security.

Peters (1999) suggests (i) the establishment and enforcement of security policies and procedures; (ii) the implementation of effective training programs for lowest-level users through systems administrators, and (iii) the refinement of network architectures and the incorporation of protection technologies (cited by Hawkins *et al*., 2000 p. 137). The establishment of security policies and procedures will prevent many occurrences of fraud at the private level. Company employee actions would be regulated by such policies and procedures, thus minimising the possibilities of fraud occurrences. Moreover, proper construction of protection technologies and network architectures would enable prevention of fraud before its likely occurrence.

The need to have effective countermeasures is obvious, given the presence of a large number of banks and financial institutions, multinational oil companies and other trading organisations in Saudi Arabia and their multi-dollar businesses connected to global business. The effectiveness of countermeasures adopted by organisations to combat online fraud is thus questioned. The impact of these countermeasures on the deterrence, prevention, detection and punishment of online fraud therefore needs to be examined. The organisation's preparedness and other influences on the countermeasures may also affect the effectiveness of the countermeasures.

This thesis therefore examines how different countermeasures in deterrence, prevention and detection in Saudi Arabia have affected the control and prevention of online fraud.

1.5 Research Question

The research focus is on the examination of the different countermeasures in the deterrence, prevention, detection and punishment of online fraud activities employed by financial institutions in Saudi Arabia, and the impact of the countermeasures individually and collectively in the control and prevention of online fraud. The research also focuses on examining the organisational / environmental context and factors that may affect the effectiveness of the countermeasures. The research questions are:

1. How have the countermeasures of deterrence, prevention, detection and punishment of online fraud activities affected the control and prevention of online fraud in Saudi Arabia?
2. What are the organisational and environmental factors that affect the effectiveness of the countermeasures?

1.6 Research Aims and Objectives

The main aim is to examine the countermeasures employed by financial institutions in Saudi Arabia and the impact of the countermeasures individually and collectively in the control and prevention of online fraud in Saudi Arabia. The research also aims to examine the organisational / environmental context and factors that may affect the effectiveness of the countermeasures. This intention is to develop a framework to help in the effective design and

development of countermeasures that would help controlling online fraud in Saudi Arabia.

1.6.1 Objectives

1. To examine the countermeasures of deterrence, prevention, detection and the remedies for online fraud in Saudi Arabia.
2. To examine the impact of the countermeasures against online fraud.
3. To examine the influence of the environment on the countermeasures and online fraud.
4. To develop a framework of deterrence, prevention, detection and remedies in terms of countermeasures against online fraud in Saudi Arabia.

1.7 The Nature of the Research

Research methodology concerns the design of an appropriate structure for investigation, with selected tools for the identification of data sources, the collection of the data, its collation and analysis and the interpretation of the results.

The objectives of this research focus on examining the countermeasures adopted by organisations to deter, prevent, detect and remedy online fraud in their environment, and the impact of these countermeasures in the context of the operating environment. These objectives suggest that the focus and nature of study is more in the nature of socio-technical rather than pure technical research, and therefore the successful fulfilment of these research objectives

requires a methodological approach fit for such research. The focus of study and the nature of the research therefore require a broader and an in-depth examination of the experiences of the participants from their own perspective, in their social and cultural context (Myers, 2009). This is to ensure and enhance a balanced coverage of the subject matter that would guarantee an easier and better understanding of the study phenomenon, all of which is essential for the effective analysis and interpretation of the data.

A qualitative method approach is therefore chosen for the investigation of the subject matter in order to obtain the optimum of the investigation and to facilitate a comprehensive knowledge of the subject matter (Creswell and Plano Clark, 2007; Newman and Benz, 1998; Bryman 2001; Sarantakos, 2005). A qualitative approach is usually designed to understand subjects and the social cultural backgrounds within their environment (Myers 2009). Using a thematic method to identify issues of concern from the data sets collected, while highlighting sub-themes and themes.

1.8 Thesis Outline

The present chapter (Chapter 1) is an introduction and background to the problem. It highlights the increasing rate of online fraud, in spite of the countermeasures put in place by organisations and the government of Saudi Arabia to control it. The chapter suggests the need to examine the measures and techniques adopted by Saudi Arabian organisations and the government, such measures to effectively control or prevent online fraud in the country.

Chapter 2 reviews the concepts of online fraud, the types and nature of online fraud, the drivers of online fraud activities, online fraud in the Gulf region and Saudi Arabia. It also reviews the countermeasures adopted by organisations to control online fraud. The chapter also highlights the various components of the different countermeasures, and suggests a framework for proper coordination of countermeasure activities. It highlights certain organisational, environmental and cultural issues that may affect the impact of the countermeasures adopted.

Chapter 3 reviews the theories that could possibly be used as a lens to examine the subject matter. It also introduces the General Deterrence Theory (GDT) as a suitable theory, because of its argument for a systematic approach in the organisation and adoption of countermeasures to control online fraud. The chapter therefore introduces a theoretical framework to be used to carry out the empirical investigation.

Chapter 4 reviews the research methodological approaches with their underlying philosophies and assumptions. It highlights the different research strategies, design methods, and suggests an appropriate approach for the research. A qualitative method approach was chosen in order to obtain a broader, in-depth examination of the experiences of the participants from their own perspective, in their social and cultural context. This was to ensure and enhance a balanced coverage of the subject matter. The chapter also introduces the chosen research design and how the data were collected and analysed.

Chapter 5 introduces and presents the qualitative data analysis, using a thematic analytical method. The chapter identifies issues of concern from the datasets collected, while highlighting the sub-themes and themes used for the interpretation of the participants' responses. The themes identified are: perception; awareness; technological measures; regulations and enforcement.

Chapter 6 brings together the highlights of the interpretations of the qualitative data in Chapters five. It highlights the important findings of the research and relates them to the existing literature.

Chapter 7 forms the conclusion derived from the discussion in Chapter six and highlights the implications of the study findings, with recommendations, limitations and future research.

1.9 Summary

This chapter has introduced online fraud and presented some background to the problem. It highlighted the increasing rate of online fraud and its possible factors. The need for adequate consideration for privacy and security issues and the use of technological infrastructures to combat online fraud was also outlined. The need to examine countermeasures and techniques adopted by Saudi organisations and government, which could effectively control or prevent online fraud in the country was also outlined. The next chapter reviews the literature on online fraud and the countermeasures required to control it.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Chapter 1 introduced online fraud as a huge and rapidly growing epidemic that has spread through most online activities (Waters, 2003). The chapter also presented some background to the problem situation, highlighting the impact of technological innovations and the adoption of online transactions such as e-commerce and e banking, the opportunities created for online fraud and the need to examine countermeasures in the control and prevention of online fraud. This chapter reviews the literature on online fraud starting with cybercrimes, types and factors driving the increase of online fraud; online fraud environments such as electronic commerce and electronic banking, the Saudi Arabia context, and the countermeasures required to control and prevent online fraud.

2.1 Cybercrimes

The increase in the dependant of business and social activities on the Internet has created virtual world which has seen the rise of cybercrime described as offences committed in the virtual environment associated with the Internet (Sandywell, 2010; Hunton, 2009). These offences range from criminal activity involving data content and copyright infringement, and more broadly fraud,

forgery and unauthorized access (Krone, 2005). Cybercrime thus describes a range of criminal activities, including ‘’computer hacking, virus attacks, fake websites, cyber-stalking, email scams and cyber-extortion’’, which are carried out using a computer and / or the Internet (Fraud Advisory Panel, 2009).

The UN (1995) identifies two main categories of cybercrime, the first category including “any illegal behaviour by means of electronic operations that target the security of computer systems and the data processed by them’’. The second category includes any illegal behaviour committed by means of, or in relation to, a computer system or network including such crimes as illegal possession and offering or distributing information by means of a computer system network ’’(United Nation Congress, 2000,p.5).

Cybercrime activities are thus designed to deceptively obtain access to a victim’s financial information for use in fraudulent activities or to misuse their devices to illegally attack other parties.
According to the platform and medium used, cybercrime can happen across a wide spectrum (Gordon & Ford, 2002), and could therefore be used as a broad term to define a subordinate of computer crime (Cross, 2008).

Cybercrime may thus be divided into two categories, the first category describing “crimes where computers are the target of the offence, and does not victimise individuals’’ (Jewkes, 2010, p. 526). The second category is conventional crimes, such as identity theft and stalking perpetrated with the aid of computer and information technologies. Cybercrime may also be categorised

according to three sets, namely white-collar crimes, non-violent crimes and violent or potentially violent crimes. Most crimes carried out online are of the non-violent type, due to the absence of physical contact between those involved. This non-physical contact and the cloud of anonymity and virtual experience provided by the Internet enable most white-collar crimes (Cross, 2008). White-collar crimes include cyber-trespass, cyber-theft, destructive cybercrimes and cyber or online fraud. Cybercriminals now adapt to social and economic changes to exploit victims in many new ways, as cyber technology develops and enables more crimes to be committed online (Garlik, 2009).

Rho (2007) refers to cybercrime as the illicit action done by a private individual or a group in cyberspace. “Cybercrime is therefore described as a criminal activity in which computers or computer networks are the principal means of committing an offence or violating laws, rules or regulations ’’ (Khsetri, 2010).

It is also described as “a range of illicit activities whose common denominator is the central role played in their perpetration by network based IT infrastructures” (Majed, 2008). They are also described as “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks” (Majed, 2008).

Kshetri (2010) identifies types of cybercrime as ‘‘ a) denial-of-service attacks, b) cyber-theft, b) cyber-trespass, c) cyber-obscenity, d) critical infrastructure attacks, e) online fraud, f) online money laundering, g) criminal use of Internet communications, h) ID fraud, i) use of computers to further traditional crimes; and j) cyber-extortions’’.

Online fraud is thus a type of cybercrime with deceptive activities using online Internet facilities. However, the following section reviews online fraud and the different types.

2.2 Online Fraud

Online fraud has the generally common deceptive characteristics of cybercrime perpetrated in a business relationship for personal gains. It is an act to intentionally deceive through false information, claim or the suppression of the truth (Albert, 2002; Brenner, 2010). Online fraud is thus generally described as the use of online facilities to carry out dubious business transactions with the intention of deceiving or defrauding persons, organisation or governments (Moore, 2014).

Online fraud has also been described as any kind of fraud scheme using any component of the Internet for fraudulent solicitations and transactions (Albert, 2002). It is perpetrated in different disguise, forms or shades, using the cover of the Internet. Common forms include online identity theft and fraud, online retail schemes and online auction fraud.

The penetration of the Internet in economies and commerce and the changes it has brought in the way business transactions are done have opened up avenues to perpetrate internet fraud or cybercrimes, as fraudsters hide behind the cover and anonymity of the internet (Moore, 2014). Online users are therefore exposed to fraudulent solicitations and transactions with the use of false documentation or identity theft.

The Internet and e-commerce have created business platforms for merchants around the globe to engage in a commerce that allows business transactions, including invoicing, payments and goods delivery to be made online, mostly in non-face-to-face transactions. However, this platform has also created opportunities for fraudulent practices online, thus creating channels for e-commerce and doing online business (Montague, 2011).

The world in general has experienced an increasing virtual attack on virtual wallets and the online accounts of citizens (Brytting, Minogue & Morino, 2011). Its prevalence has been noted to be in regions where there is high adoption of e-commerce, with large online financial transactions. Online fraudsters have therefore perpetrated their fraudulent practices in online banking, auction trading and e-commerce to earn dubious money, while victimising online users or employees (Deloitte, 2011; Hawkins, Yen & Chou, 2000).

The occurrences of online fraud have benefited from the nature of online transactions which enables transactions between two or more parties irrespective of the physical presence of the players but allows instructions through an online medium. This has enabled the use of false documents and false identity on online transactions such as electronic commerce (Wall & Williams, 2014). Unfortunately the expansion of electronic commerce is increasing rapidly with retail online transactions reaching about $268 billion in 2012 (javelin strategy and research, 2008). These varieties of cyber-crime show the different avenues for online crime and the different ways online fraud may affect businesses and the economy in general. This also implies that the

prevention and detection of all these varieties may require different approaches and countermeasures in order to successfully combat online fraud.

The Internet Crime Complaints Centre (ICCC) received about 262,813 complaints in 2013, most of which concerned non-delivery of payments / merchandise, FBI-related frauds and identity theft, costing the victims millions of US dollars as total losses (IC3, 2013). Also Microsoft (2012) stated that ‘‘online fraud victimises millions of unsuspecting people every year with an adjusted loss of nearly half a billion dollars’’ (p .2).

Online fraud is therefore increasingly becoming a problem and a major challenge to organisations and governments globally, particularly in the Gulf region (GCC), where there has been a vast number of financial transactions carried out online, aided by high acceptance and the penetration of internet technology in the region (Stringham, 2005; El-Guindy, 2008). Online fraud has reached an alarming rate worldwide, therefore combatting, controlling and preventing it has become a major challenge (Coyne, 2005; Montague, 2011). Governments and organisations have made efforts to control the rate of online fraud, but measures put in place may have yielded little or no success, as the rate of online fraud still remains high (Higgins, 2009).

The Internet due to its varieties of uses such as for electronic commerce has thus become a platform for online fraud and other cybercrimes (Clifford, 2011). Electronic commerce using the Internet therefore presents potential problems for online users at both personal and business levels (Stringham, 2005). The

ever-expanding connections enabled by the Internet are seen also to attract the possibility of significant losses through online fraud, which could be a major threat to electronic commerce (Coyne, 2005). It is argued that most dealers are tending to evolve more complex means of prevention (Montague, 2011) and use fraud in e-commerce as a method of doing business.

2.3 Types of Online Fraud

Online frauds are of different dimensions, intents and forms with varying effects on e-commerce. The dimensions of online fraud include miscellaneous fraud, Advance fee fraud, online auction fraud, phishing and online investment fraud. Miscellaneous fraud is where a variety of scams are intended to defraud the public, such as “work-at-home scams, fraudulent sweepstakes and contests, and other fraudulent schemes” (ICCC Report, 2010, p. 18). Various websites have set up bogus websites and contests or sales, requesting unsuspecting consumers to register with a fee and detailed personal information, all in the aim of duping them out of their monies and information.

Advance fee fraud occurs when “criminals convince victims to pay a fee to receive something of value, but do not deliver anything of value to the victim” (ICCC Report, 2010, p. 18). The consumers are presented with fake documents, identity and claims of some valuable resources that the consumer may desperately want. Auction fraud is where fraudulent transactions occur in the context of an online auction site (ICCC Report, 2010, p. 18).

Overpayment fraud is “incident[s] in which the complainant receives an invalid monetary instrument with instructions to make a deposit in a bank account and return excess funds or a percentage of the deposited money back to the sender” (ICCC Report, 2010, p. 18).

However, three main types of online fraud are common in relation to the context of this study; these include online auction fraud, phishing and online investment fraud. The next section examines these types of online fraud.

2.3.1 Online Auction Fraud

One widespread variety of fraud is online auction fraud. Online auction fraud is a type of fraud that mostly affects consumers through the bidding process for goods and products carried out online. It is noted that online auction fraud has risen tremendously from 106 cases in 1997 to around 24,000 in 2007 and is continuing to rise dramatically (Reuters, 2003). It represents a clear and imminent threat to the financial stability and welfare of ordinary customers, but also to companies and financial institutions (Moore, 2014). Many auction houses therefore now pay attention to the menace of online auction fraud perpetrated by bogus and dubious sellers, as many people are now losing confidence in the online auction system (Palmer, 2005).

The significance of this type of fraud is highlighted, that it is ranked in the Top 10 Complained Crimes in The Internet Crime Complaint Centre (IC3), which is an organisation trusted by the Federal Bureau of Investigation (FBI) for tracking Internet crime. Online auction fraud is regarded as one of the main overall

sources of Internet fraud, with occurrences estimated to be from 64% to 87% of all Internet fraud (eMarketer, 2001; ICCC, 2007). This variety of fraud is usually committed via online auction sites, such as eBay. Such sites bring over a hundred millions items together for sale, with multiple sellers and buyers. The sales usually include sales of goods, such as cars, clothes, consumer electronics, books, movies, music, antiques and so on. Some sellers fail to send the goods paid for by the buyers or sometimes send goods other than those advertised on the websites.

It is also interesting to note that the owners of auction sites continue to deny that online fraud is a major concern for them and their users. In 2005, it was claimed by eBay representatives in the USA that online fraud represents only 0.1% of transactions using eBay sites (Cha, 2005). In numerical terms, that is approximately 3,000 fraudulent misconducts every day. However, in the opinion of the law enforcement agencies, the seriousness of online fraud on auction sites has been significantly underestimated (Shavers, 2013). Moreover, these sites create convenient conditions for committing fraud online. Auction sites are also used as platforms for the sale of stolen goods. (Yar, 2006).

They are also used to hold back goods or sell goods that do not exist, and this non-delivery type of fraud is said to constitute over 67.3 % of online frauds in the USA (McQuade III, 2005). Typically, the scheme seems to work as follows: bidders who participate on auction sales are informed usually that they have won the auction and are asked to pay money; however, after payment they do not receive the items paid for. Fraudsters of this type are not easy to catch,

because they usually use fake identities and register on sites under bogus identities, thereby confusing customers and the law enforcement authorities (Curry, 2005, p. 2). Another common variety of fraud used on auction sites is sale of goods that misrepresent their true value or authenticity (Gragido & Pirc, 2011). The misrepresentation can take several forms, one of which is to attribute “inflated retail values to items, so as to represent the auction prices as substantial savings; it may also involve misrepresenting the condition of the item as new, or items in poor working condition are advertised as fully functional” (Fried, 2001, p. 4). Fraudsters also sell counterfeit goods, stating that they are authentic items, which, for example, include such items as “counterfeit DVDs, CDs, and computer software packages, as well as counterfeit clothing, perfumes and other items” (Enos, 2000; MPAA, 2003, p. 3).

Another form of fraud on auction sites, which is difficult not only to trace but also to prove, is ‘’shill bidding’’, whereby a fraudster simulates the price of goods on an auction by placing false bids (Brenner, 2012). This is done by using multiple fake identities or conspiring with another fraudster to cooperate on multiple bidding simultaneously. The fraudster, who pretends as a bidder but with no intention to buy, pulls out of the bidding when the bid reaches a desired price after deceitfully luring other unsuspecting bidders to bid at that higher price. However, it should be noted that the percentage of ‘shilling’ frauds represents only a small proportion of auction frauds (Holt, 2012). Fee stacking is also a common variety of fraud, which, even though easy to trace, is difficult to prove. Fee stacking occurs when a fraudster adds on additional costs or fees after an auction has been completed, thus increasing the value of goods or

failing to deliver. He/she refunds the actual cost of the goods but retains the additional fee (Wall & Williams, 2014). Curry (2005) terms such common types of fee stacking frauds as ‘administration costs’ or ‘buy and switch’, where a winning bidder will swap the purchased item for a damaged, but otherwise identical item. They have already claimed a refund, and end up with both the undamaged item and their money, while the seller is left with damaged goods (pp. 2-3).

2.3.2 Phishing

Phishing is probably the most common and widespread variety of online fraud. It takes the form of various dubious and fake emails or websites, which are meant to induce users to disclose their bank accounts or the passwords to their accounts, which can be used to debit their account (McQuade, 2009). There are two common types of phishing, namely phishing itself and spoofing (McQuade, 2009). The difference between phishing and spoofing is that the latter uses fake versions of legitimate websites, whereas phishing is carried out by means of emails.

Phishing, of the first kind, is carried out more often than the second kind, because emails are easy to handle and do not require significant financial expenses, whereas the former kind requires considerable effort to maintain (Albrecht et al., 2011). The emails that the fraudster sends for phishing purposes are sent on behalf of banks, credit card companies or e-shops, where they request either to change or update their account defaults, be it a bank account or an electronic account (Albrecht et al., 2011). The texts of these

phishing emails are persuasive, inducing the victim to believe in their origin (McQuade, 2009). In order to increase user belief, logos and hyperlinks to companies are used, and, when a user “buys” such links and proceeds through the website, it mirrors the original, where he or she was asked to enter personal details, password or change them. Once they do that, the fraudsters take advantage and use them for their malicious ends.

2.3.3 Online Investment Frauds

Online investment fraud or simply investment fraud is a rather sophisticated type of online fraud, because it requires a certain level of knowledge about finance and accounting (Brenner, 2010). A person with a basic knowledge of finance can be the victim of this type of fraud. It is usually perpetrated using several modes. The first and common is where investments are invited into non-existent companies or enterprises (Clifford, 2011). What fraudsters often do is to persuade online users to invest in one or several non-existent companies located abroad (English, 1996). Alternatively, fraudsters offer online users the purchase of shares in a non-existent company or firm.

Fraudsters use mass emails, online investment newsletters, bulletin boards and chat rooms in order to attract customers (Beresford, 2003). They employ a scheme known as ‘pump-and-dump’, where a person contacts another person claiming to have ‘inside information’ about a stock-market listed company about which only he has information (Beresford, 2003). This induces that person to buy stocks in the company, because he or she expects a good and rapid income (Yar, 2006). With the new high price, the perpetrator ‘dumps’ his or her

own stock in the company in order to cash in on the temporary rise (Fried, 2001, p. 6). After the failure of such a scheme, the price of the stock goes down and the fraudster gains profit at the expense of the deceived customers (Beresford, 2003).

This is a common scheme for online fraudsters normally carried out either online or by phone, but the online fraud mode is mostly preferred. Unfortunately, this kind of scheme also works in the Arab world, and especially in the Saudi Arabian Stock Market, despite ethical and religious restraints. It is important to keep in mind that *Sharia* outlaws these kinds of dealings and regards them as sinful. Despite this, because of the promise of high returns, most people become victims, and do not feel restrained themselves by the ethical rules of Sharia or any social norms.

2.3.4 Online fraud Concept in this Research

Online fraud is defined for the purpose of this research as any use of online facilities to wrongfully and criminally deceive or defraud persons, organisation or governments for personal financial gains. It is regarded as a deliberate misrepresentation of facts or documents in financial transactions with the aim of fraudulently obtaining money or other assets from a bank. It is also defined as criminal exploitation of the e-banking/e-commerce media and platform and taking advantage of the weaknesses in the internal control systems (Adams, 2010; WiseGeek, 2013). The focus of this research based on this definition of online fraud is therefore fraud perpetrated through the e-commerce and e-

banking systems in financial transactions. The Banks, online bank frauds and staffs and victims will therefore form main participants in the study investigation.

2.4 Electronic Commerce

Electronic Commerce (EC) is a platform that combines information and communication technologies with other infrastructures and standard procedures and processes to bring buyers to interact with sellers and in exchange of goods and services (Mann, 2000). Electronic commerce is therefore a platform for online business transactions using the Internet and other telecommunication infrastructures. Thus, e-commerce is online business transactions which include all activities to conclude sales, driven and enhanced by computing and Internet technologies (Whiteley 2000; Chaffey 2004). The businesses transactions may include pre-sales activities such as making orders, checking of catalogues, prices, payments, etc, and also include post-sale activities such as deliveries, invoicing, refunds, etc.

In the past decade, there have been great improvement and adoption of Internet infrastructures in both the developing and developed countries but with a comparatively different success rates among different countries, with various issues such as online fraud. This implies that the development of e-commerce may not depend on just only infrastructural developments but other factors as well. It is therefore suggests that the effective use of E-commerce requires three kinds of infrastructures namely the infrastructure of technologies necessary to create the market platform; process infrastructure required to

create necessary connections and transactions such as payments and methods of goods delivery, and; the platforms of protocols which highlights common and standard laws and regulations that would regulate business transactions between all parties (Mann, 2000). Having these infrastructures in place may help avoid most problems associated with e-commerce such as online fraud.

The effective use of e-commerce in some countries and regions particularly the developing countries has however been hindered by lack of protocols, inadequate processes and relevant regulations even though there may be adequate Internet facilities (Rahman, 2009). The deficiency of Internet access and technological infrastructure may not be the only factors effecting the development of E-commerce in developing countries. The issues may be in the platform of protocols and processes required to augment and compliment the available technologies (Rahman, 2009). This process infrastructure and the infrastructure of protocol regulate transactions in e-commerce and therefore may determine the level of security and its success. The process infrastructure which deals with payment and delivery arrangements needs to be authentic, secured and reliable. Most vulnerable e-commerce customers have been defrauded or deceived into paying into fake accounts, or pay for goods but never get the goods delivered. E-commerce has therefore experienced all kinds of fraudulent activities that have exploited the process infrastructures. The Internet by nature allows for anonymous payments which may have provided avenues for fraudulent activities. While processes are introduced to make payments easier and faster, such as the use of credit and debit cards for

online purchases, more opportunities may also have been created for online fraud.

E-commerce with the introduction of advanced technological innovations has brought changes in business practices (Brodie et al, 2007; Gonza´lez et al, 2008), and business organisations constantly develop strategies alongside the changing technologies to enable them expand their customer base and business network by effective and easy delivery of products and services while ensuring transaction security. E-commerce may therefore depend more on trust in the security of the transactions which can be assured through the process infrastructure and the infrastructure of protocols. The consumer may always have doubt and fear of the possibility of their card details used fraudulently or the fear that goods ordered may not be delivered. The increasing number of concerns for fraud and actual fraudulent practices in E-commerce may also be affecting the acceptance of E-commerce by many customers who have refused to shop online.

The rapid advances of electronic commerce are efforts focused on encouraging electronic society which relies on the use of credit / debit cards or other electronic medium for purchases and other electronic transactions. The focus is convenience and cost effectiveness which also may depend on processes and protocols. The use of these credit and debit cards are done in two major ways namely physical cards where the cardholder presents the card at the point of sales for payment requiring pin numbers, and virtual card usually used in online purchases where only some necessary card details such as card number, expiration date, and secure code are requested for in making payments. The

possibility of fraud thus increases as the use of cards in e-commerce transactions increases (Falaki, *et al*., 2012).

It is noted that the UK, Spain and France have about 322 million credit and debit cards in circulation, while Germany has about 92 million. This growing number of users and their transactions thus creates the avenues for online fraudsters to perpetrate crimes (Falaki *et al.,* 2012). The growth rate of e-commerce transaction fraud and the evolving nature of online fraud is forcing merchants to establish fraud prevention measures which may depend on laws defining online fraud and its consequences.

The infrastructure of protocols, which focuses on required laws and regulations to conduct the activities of all the players in the market, is thus required to protect both the customers and the organisations involved in e-commerce (Mann, 2000). The Council of Europe's Convention on Cybercrime (2001) has made efforts to creating common laws in the EU which would provide the platform to combat crime in e-commerce, however, the Convention has been criticized for laying much emphasis on the economic interest of organisations and governments avoiding individual users. The laws do not also take into accounts privacy rights or data protection issues (Jewkes, 2010). The Metropolitan Police (2008) note that the Internet enables new methods of transacting business for both the law-abiding and the law-breaking parties, and it is therefore imperative that every care should be taken in order to ensure that the competitive advantage of e-commerce does not favour illegal activities (Hunton, 2009. Therefore, the e-commerce platform eliminates the need for

face-to-face communication, thereby reducing the level of anonymity usually exploited by criminals. According to Fletcher (2007), ‘‘the lack of face-to-face communication and reduced level of anonymity also reduces the perception of risk but increases the appearance of legitimacy to the potential victim’’. The platform thus provides a simplified, cost effective and repeatable means of carrying out attacks against a global cyber-community, about 3.6 million criminal acts being performed online (one every 10 seconds in 2008) (Bryant, 2008; Garlik, 2009). This is a clear threat to the Internet and there are calls for prompt technical and legal action to gain control and reinstate confidence in the platform and in e-commerce (Hache and Ryder, 2011).

Generally the Arab world, has experienced slow e-commerce development due to lack of an adequate ICT infrastructure, and trust issues, which results in the absence of clear rules and regulations, as to how to protect the rights of those involved (Al-Solbi and Mayhew, 2005; CITC, 2006; Alfuraih, 2008; Alraw and Sabry, 2009 and Alghaith, Sanzogni and Sandhu, 2010). It is estimated that the rate of retail online transactions will double across the whole world (Javelin Strategy and Research, 2008). Moreover, the use of online services such as shopping and trading has contributed around $ 1.5 trillion to the e commerce industry globally (Criteo, 2015). Relatively Saudi Arabia has the most rapid and expanding growth of ICT marketplaces within the Arab region, although of e-commerce activities and e banking are not advancing at the same ratio (Alfuraih, 2008; CITC, 2007).

The following section looks at the popular growth of electronic banking services and the security issue concerns.

2.5 Electronic Banking

E-banking is described as banking services provided through a new delivery channel, namely the Internet (Financial Services Authority, 2000). Electronic banking services are a class of banking services offered by banks to individuals and corporate institutions using various electronic means, (RATIU, 2011).

These newly evolving e-banking services differ considerably from the previous services, which usually take place within the four walls of the bank's offices (Khan and Mahapatra, 2009). The most popular types of E-Banking services include Online Banking, ''Automated Teller Machines (ATM), Electronic Funds Transfer, Electronic Cheque Conversion, Direct Payment and Web ATM services''. Because of the cheap and fast nature of the e-banking delivery channels, banks have globally continued to shift to the adoption of e-banking, to the benefit of their customers (Sathye, 1999; Tero Pikkarainen, 2004).

However, these new E-banking services and delivery channels come with some security challenges, especially with all banks turning to e-banking and with the increased access of millions of bank customers to increased financial transactions. There are several security and other operational issues related to these services and delivery channels. The issues may include the deficient legal framework and security issues that surround electronic transactions, which strain the ever-expanding process.

The challenges posed by the increased adoption and use of e-banking vary from financial limitations and the reluctance to adapt to new technological systems, as well as an increase in security fears, cultural barriers, restrained

Internet access and legislation (Masocha, 2011; Auta, 2010). Thus, security, the lack of it or its inadequacy, is a major issue in e-Banking, and could, potentially lead to monetary losses, fines imposed by regulators and bad media coverage (Shah et al, 2013). It is also noted that the platform of e-Banking, where large transactions can be made anonymously and where claims cannot be effectively verified at the point of sale, offer incentives for fraud (Roberds, 1998). These incentives need to be considered more carefully, and managed to reduce the potential for online fraud.

Adams (2010) notes that banking fraud is described as the ‘’wrongful or criminal deception that results in financial or personal gains’’, and could be attributed to the majority of financial institutions’ losses. Criminals exploit the e-banking media and the weaknesses in the internal control systems utilised to commit crimes (such as online banking, cheque and card fraud) (CBN Annual Report, 2010). Most fraud cases committed in 2010 were perpetuated through the transparent platform of electronic banking systems (CBN Annual Report, 2010).

Bank Fraud is therefore described as the use of deliberate misrepresentation, a criminal deception with the aim of fraudulently obtaining money or other assets from a bank (wiseGeek, 2013). This criminal deception has taken different forms and shapes, including sales fraud, purchase fraud, cheque payment fraud and many others (Benjamin, 2011). Both individuals and organisations, especially small and medium-sized organisations have had their bank accounts hijacked and drained by cybercriminals over the past decades, using sophisticated malware and phishing emails. Ponemon (2011) in a study of e-banking fraud noted that 48% of SMEs(small and medium enterprise) in the

US claimed that they experienced e-banking fraud two to five times in a period of twelve months, while 38% experienced it once in twelve months, 15% experienced it six to ten times and 3% experienced it more than ten times. The report also noted the consequences of e-banking, which shows that 43% of the customers who were duped or experienced e-banking negatively moved their businesses to other more secure banks, while 26% of the customers lost confidence and trust in the bank's online security. The report also showed that banks failed to detect online fraud in 78% of the cases. The study also noted that the responsibility for combating online fraud lies with the banks, (70%), customers (15%), government regulators (10%) stake and law enforcement agencies (5%).

The report of the survey of 533 SMBs therefore implies that the industry has made little headway in tackling the issue (Ponemon, 2011). A good success may require the collective approach of all stakeholders to fully combat online fraud. Existing anti-fraud measures by banks and governments have not been able to make much progress, and stakeholders are constantly considering new security measures aimed at eradicating e-banking fraud (Roberds, 1998). Various studies have also shown the need for improved authentication systems, as the conventional methods of authentication via usernames and passwords, which increase the vulnerability of customers, are no longer sufficient (Robert *et al*., 2009; Vandommele, 2010).

It has also been noted that most cases of e-banking fraud were committed with the collaboration of those security and bank officials who had direct access to banking systems and access to customers' personal information and records (Aransiola, 2011). The employees of banks therefore exploited the loopholes in

the banks' internal control systems and misused their privileged positions, thereby compounding the threat of e-banking fraud and adding a different dimension to its motives, compromising the relevant countermeasures (Sidden, 2005; Benjamin, 2011). This dimension of collusion with internal bank personnel highlights the importance of other factors other than technology in combating the threats of online fraud.

The Gartner Group (2009) reported that, with the existing countermeasures, cyber criminals are winning the cyber war against financial institutions, thus making online banking unsafe, as long as the banks fail to take corrective actions and effective countermeasures. Therefore, it brings into question as to whether banks adequately prepared to combat online fraud.

2.5.1 Security Challenges in E-Banking

Researchers have noted that e-banking fraud takes on different forms, but mainly through online crimes and identity / card theft. Moreover, e-banking fraud usually is committed due to compromises in security, stretching from weak authentication systems to insufficient internal controls. This implies that e-banking fraud emanates from two main sources, namely technological and the organisational and social environment. Securing e-banking therefore requires factors beyond technology to be addressed. Other factors including internal controls, customer education and staff education need to be considered alongside technological issues (Usman and Shah, 2013). The identification and understanding of these critical success factors could be crucial in enhancing fraud prevention systems in e- banking.

Technologically, the two critical success factors are: Appropriate technical fraud prevention measures and innovative use of fraud prevention technologies (Usman and Shah, 2013). These factors usually aim to manage the issues of identification, authentication and non-repudiation of information security, and can be very instrumental in reducing or eradicating e-banking fraud (Bhattacharyya, 2009). Notable and increasingly popular technological innovation is the biometric technology for biometric authentication of identities, using techniques such as fingerprint and keystroke dynamics (Murdoch, 2010). However, false rejection and acceptance rates and the cost of deploying such a technology in most banks have featured prominently in making a case against it.

Another non-technological critical factor is customer vulnerability to fraud, which is affected by factors such as education and awareness (Choplin, 2011). Behavioural patterns also show the vulnerabilities in the human component of any complex system, not merely opportunities for small-scale hustles. This implies that the most vulnerable aspect in any security-strengthened system is usually its human element, and therefore real-world systems may be vulnerable to attack in spite of protection by elaborate technical safeguards.

A robust online fraud security solution and measures may therefore require acknowledgement of the existence of these vulnerabilities as an unavoidable result of human nature **(**Stajano and Wilson, 2011).

It has been suggested that blind ambition is at the heart of very many fraud scenarios, as users focus on obtaining what they want at all costs, and are easily distracted from the task of protecting themselves, thereby creating opportunities for fraudsters. Obtaining easy access to what users want usually

makes them display a negative attitude to the security processes and procedures designed to protect them. Countermeasures and security systems therefore need to understand and work with this principle, as access control to sensitive databases may involve an exploitable human element (Stajano and Wilson, 2011).

Other user behaviour and principles that reflect the vulnerabilities of users include the social compliance principle, which makes users suspend their suspiciousness, leading them to be exploited by fraudsters. The herd principle makes users to drop their guards, as they see everyone around them behaving in similar ways; the need and greed Principle, where the needs and desires of users make them vulnerable to manipulation by fraudsters; and the dishonesty and kindness principles.

Countermeasures for online fraud or any system involving people may only be more secure and effective if the inherent vulnerabilities of the human factor are acknowledged, understood and considered in the design of the countermeasures. The critical factor therefore is that people need to be aware how various Internet usage behaviours can result in making them vulnerable and exposed, and how changing their behaviours can simply provide more protection.

Another critical approach banks are taking is to alter the focus of customer authentication from authenticating the user to trying to monitor their activity to track unusual behaviours. This involves profiling customers' transactions and usage habits to flag unusual activity and intercept a fraudulent transaction. Improved knowledge of their customers may therefore be required for banks to

provide security systems and countermeasures to online fraud (Brian Krebs, in KrebsOnSecurity.com).

Another key issue is making the E-banking consumers feel safe and convinced of the ability and effectiveness of the countermeasures against online fraud. More users would want to be informed by their banks about fraud prevention, and steps taken to combat fraud. Consumers are increasingly concerned about security, the privacy of their information and the rising rate of fraud, and would therefore feel better and more secure with the establishment of fraud resolution programs by banks. Rizzardi (2008) is of the opinion that customer education is very important in helping to protect their identities to prevent payment card fraud.

2.6 Online fraud in Gulf Cooperation Council (GCC) Region

The Gulf Cooperation Council (GCC) was established as a cooperative organisation on May 25th, 1981, with the aim of solving issues arising out of economic, financial and trade areas in the Gulf region (Ramady, 2014). It is an economic cooperation organisation bringing together countries in the region that have different levels of economic development, but the same language, culture and religion (Ramady, 2014). For example, countries like Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates are all involved in GCC activities. The majority of the GCC countries are equipped in terms of online commercial transactions (Abdallah & Albadri, 2010). However, the table below shows the increase of the Internet penetration in regards to electronic commerce in the GCC.

GCC countries	Population	2011 Est.	Users in	Dec/2011	Internet Usage
Bahrain	1,214,705	40,000	649,300	53.5 %	0.9 %
Kuwait	2,595,628	150,000	1,100,000	42.4 %	1.5 %
Oman	3,027,959	90,000	1,465,000	48.4 %	2.0 %
Qatar	848,016	30,000	563,800	66.5 %	0.8 %
Saudi Arabia	26,131,703	200,000	11,400,000	43.6 %	15.7 %
United Arab Emirates	5,148,664	735,000	3,555,100	69.0 %	4.9 %

Table3 Internet Use in GCC Internet Use / Penetration in GCC (Source – Miniwatts Marketing Group, 2011).

Internet penetration and usage in countries in the GCC area is regarded to be high ranging from 42.4% in Kuwait, 43.6% in Saudi Arabia to 69% in UAE and 66.5% in Qatar (table 2), (Miniwatts, 2011). This high Internet penetration, coupled with a changing customer profile, positioned banks in the area for more e-commerce and e-banking transactions. Banks in the area are massively promoting e-banking in different channels, encouraging customers, mostly young clients between the ages of 21 and 40 years, who represent about 60% of banking customers. The volume of online banking transactions has also been on the increase, owing to changing online behaviour, with customers now preferring online transactions. Online services have also tripled in the last decade, making the GCC region the fastest growing region in online services (Kearney, 2013). However, the main challenges in the GCC region are

customer awareness and trust in the online system which has kept older and wealthier customers away from online banking and e-commerce transactions.

2.7 Factors affecting the growth of cybercrime in GCC countries

In terms of growth in the user base, El-Guindy (2008) asserts that the number of online users has been outpacing the number of users in the rest of the world. It is further argued that, with the growing numbers of users, the level of potential abuse has also increased. A survey of Internet usage and ecommerce activities in the GCC placed the UAE first in the rate of annual spending on e-commerce per capita, while Saudi Arabia the first in the overall money spent on e-commerce activities in the region. Another major factor is the lack of security awareness in online associated business transactions in the Middle East. Most organisations in the region have invested in information infrastructure, but it has been noted that, despite the opinion that the financial institutions in the Middle East have employed the best online security systems, there has been a growing tendency for organised cyber-crime to operate via online transactions (Abdallah & Albadri, 2010).

This finding illustrates the vulnerability, even of seemingly invincible and powerful security systems. El-Guindy (2008) also touches upon the issue of investment in information infrastructure, which is particularly important for online security protection. He stated that most investments are directed at the development of e-business, but not its security. Although there have been high investment in IT infrastructures, most organisations and the public still lack

awareness of the importance of security in online business (Stavroulakis & Stamp, 2010).

One factor that may be contributing to the lack of security awareness, or the ineffectiveness of security procedures, is language differences in the security packages developed from Western countries. This could be a major barrier, as English language is not popular in the region (El-Guindy, 2008).

The majority of IT decision makers in the Arab world simply ignore online security problems and issues by pretending that companies in Saudi Arabia are immune to cyber-crime (Abdallah & Albadri, 2010). The assumption of companies' immunity to cyber-crime in the Gulf region may also have contributed to the lack of awareness and the growth of online fraud in the region (Ramady, 2014). Fraudsters have therefore exploited this situation to their own gain. Another major issue is the lack of efficient online security policies by companies, as they ignore the importance of online security in the prioritising of their business interests (Abdallah & Albadri, 2010). This in turn leads to minimisation of secure space in the e-business world of the Middle East. Poor security awareness is also realised in terms of growth in the number of cyber-criminals who abuse the ignorance and poor awareness of local users and use them as recipients of scams (Abdallah & Albadri, 2010). This seems to be an important factor, since it directly affects the rate of cyber-crime and leads on to new ones.

There is also the threat of cybercrime through social networking (Jøsang, Audun et al., 2007). Social networks are open backdoors into corporate IT platforms, because they use in daily basis by most employees (Tiller & O'Hanley, 2013). More surprisingly, hackers in the Middle East have been taking advantage of international social networks in order to infiltrate their cyber-criminal activities in the Middle East. Unemployment is also noted as one of the challenging factors affecting the growth of cyber-crime in the Middle East (Schiffbauer et al., 2014). It is a crucial problem particularly in the region as governments attempt to generate millions of jobs (Schiffbauer et al., 2014).

In terms of the lack of training in law enforcement, it seems that law enforcement in a country such as Saudi Arabia is not capable of dealing with cyber-crimes such as online fraud, because they do not understand its essence in order to combat it (Abdallah & Albadri, 2010). Moreover, most laws are political rather than legal in character. Therefore, users have been punished for their political views, ignoring real online fraudulence. Another problem faced by government agencies and law enforcement bodies in the GCC in general is the lack of technology and specialists, which has made online fraud cases reported to the law enforcement agencies increasingly a burden and thus difficult to detect or prevent (Salazar & Low, 2011). The lack of special regulation and effective enforcement agencies in the region may also have contributed to the high rate of online fraud in the region. Governments have responded by introducing a variety of measures, including criminal sanctions against trespassers, but this has not been effective. Even the adoption of a religious legislative instrument such as *Sharia* law has not done much to resolve the crisis of online fraud (Ballantyne, 1986; Elniam, 2013). This may be due to the

lack of awareness on the part of religious leaders and their followers who are required to preach and enforce the law.

Other issues, which may have affected the growth of online fraud in the region, include the quest for financial gain and getting rich ambitions of groups particularly in the face of the recent Arab spring and extremist Islamic movements. Financial gain and financial supremacy are thus described as major motivation for cyber-crimes in the Middle East (Abdallah & Albadri, 2010). The quest for financial gain may be due to the low income, lack of employment and the unsatisfactory level of economic development in some parts of the region that may have pushed many people into cyber-crime and other fraudulent acts. It is therefore important to note that, these issues and the motivating factors behind them are crucial in gaining understanding of online fraud in the region and in helping policy makers in formulating and implementing appropriate countermeasures to positively and effectively combat online fraud (Abdallah & Albadri, 2010). Although it is been noted that Cyber-crime in the region may be associated with terrorism fuelled mainly by on-going conflicts between Israel and Palestine and by religious uprising, it is a direct threat to state security but less of personal or business attack and online fraud (El-Guindy, 2008).

2.8 Cybercrime / Online Fraud in Saudi Arabia

Saudi Arabia relatively in the region has a large number of banks and financial institutions, multinational oil companies and other trading organisations, with multi-dollar businesses connected globally (Ramady, 2014). Moreover, Saudi

Arabia has the highest rate of Internet penetration, supported by government policies and the use of advanced technologies in most areas of governance and commerce. It has the highest number of Internet users with a 62.97% penetration level (Abdallah & Albadri, 2010). It is estimated that Internet users in Saudi Arabia represent 54, 2 % of the population, and the number of users are expected to increase significantly in the near future (CITC annual report, 2013).

These expansion of businesses, global trade connections and increased online activities have however been accompanied by a surge in Cybercrime/online fraud in Saudi Arabia, costing the country SR 2.6 billion in 2012 (arabnews, 2012). Several cases of online fraud have come to light with serious implications to the country's and regional economy, its rapid expansion and widespread penetration into all the sectors of the economy, in a short period of time, is making online fraud more complex to handle. For example, in 2013, one of the largest oil companies in the world (Aramco) was targeted by cybercrime attacks, which resulted in the destruction of about 30000 computers including valuable data. Many other government's websites have also been targeted and attacked in the past decade due to the widespread use of the Internet in the region (world exchange report, 2013; Al Arabiya news, 2013).

In relation to online fraud, the most common form of online fraud in Saudi Arabia is centred on the use of credit / debit cards. It is reported that majority of the online frauds involve the absence of authorization and cancellation of

authorisation. Other concerns are non-recognition of transactions, payment by other means and double charges.

It is therefore argued that the rate and nature of online fraud in Saudi Arabia may be higher by comparison to others in the region, because of the level of the organisations involved and the security measures taken to deter and prevent fraud (Ramady, 2014). The government's efforts to put in place necessary policies and regulations to enhance the sustained positive use of online transactions may also have inadvertently contributed to the high level and nature of online fraud in the country as online fraudsters take advantage of the government's provision of internet infrastructures and other facilities (Ramady, 2014).

In addition, the King Abdulaziz City for Science & Technology (KACST) is responsible for overseeing Internet services in Saudi Arabia, which includes the implementation of government censorship through the government's Internet Services Unit (ISU) (Ramady, 2014). In January 2008, the government through KACST introduced some 16 articles of laws and regulations establishing codes of practices and use of the Internet both for personal and business purposes. The laws prohibited certain uses of the Internet such as for pornography, illicit trading, government attacks, etc. The laws stipulated punishments for prescribed offences and proscribed activities (Internet Filtering in Saudi Arabia, 2009). ''The law stipulates penalties not only for online fraudsters but also for accomplices, and even those who are proven to have only the intent to engage in unlawful IT acts'' (opennet Initiative, 2009e, p. 3).

However, It should be noted that the techniques used by online fraudsters is consistently changing and adapting to the latest trend and very difficult to proactively combat it in Saudi Arabia. However, Ahmed et al. (2011) identified some measures that may be used effectively to combat online fraud. These include: (i) SMS information security; (ii) biometrics information security; (iii) token-based information security mechanisms; (iv) access control list (ACL); and (v) digital signature information security mechanisms.

2.9 Fraud Prevention and Detection Techniques

The varieties of online fraud and the different techniques used by online fraudsters have also necessitated the invention of different prevention and detection techniques to arrest the negative effect of online fraud. However, the techniques adopted to combat online fraud are dependent on technological innovations and their acceptance and effective use in organisations. While some techniques are easy to use and effective in some areas, some techniques may have been found to be difficult and inappropriate to use in some areas and culture. The different techniques are thus designed for specific purposes such as identity checks, cheque verification and address checks, and may be applied manually or with the use of technologies. The different techniques, purposes and technological applications will be discussed in this section.

2.10 Methods of Identity Proof

Identity theft is a major avenue for online fraud and therefore most of the fraud prevention and detection techniques are based on verifying the correct identity

of the user in every online transaction. The identity of the user can be confirmed in many ways using different information of the user such as address, age, and date of birth, etc. These details of the user may be confirmed by telephone calls, email or by electronic means. This section discusses the use of user's details to confirm identity.

2.10.1 Address Verification Systems

Address verification systems (AVS) is designed to confirm the authenticity of the address of the user. The registered address of the user in the user's bank details needs to conform to the address given by the user. The system can be effective in protecting users against credit card fraud conducted online (Biegelman & Bartow, 2012). The system allows a purchaser to check whether a submitted email address is with the bank that issued the card (Spann, 2013). It is used as a constituent part of the credit card security system, and supported in such countries as the United States, Canada, and the United Kingdom (Montague, 2011), and is covered by such systems. The AVS can only prove itself effective in the context of Saudi Arabia if a secured connection is provided in an Internet network within the country. It may be plausible only when full Internet security and countermeasures are assured within the network.

2.10.2 Advanced Address Verification

Advanced address verification system (AAV+) is more sophisticated to AVS; it uses a combination of addresses in multiple databases to confirm the address of the user. It can be used to check the "billing address on file with what the cardholder provided to also check the shipping address, e-mail address, and phone number" (Montague, 2011, p. 132). However, the system is only used by

American Express, and may not be useful when other credit cards are used in online transactions (Spann, 2013).

2.10.3 Age Verification

Age verification is commonly used to check the user's age at the time of purchase, usually used in combination of other user's identity information and in sites and transactions where the age allowed to purchase the products being sold need to be checked e.g. the sale of alcohol, and the adult and gaming sectors (Black & Ferguson, 2011). For religious reasons, such issues as alcohol, adult movies and gambling, are prohibited in some countries of the GCC, with the exception of Bahrain, Qatar and UAE. It can therefore be suggested that this type of fraud will not be relevant to most users, simply because such sites are banned in these countries.

2.10.4 Card Security Schemes

The checking of Card Verification Value (CVV) numbers unique to every card also ensures the identity of the cardholder and the card used for the online transactions. It is a way to confirm that the person claiming to be the owner of the card is with the card and is the actual owner (Biegelman & Bartow, 2012). However, this is usually used together with other details of the cardholder such as the address. It is the best way to prevent credit card frauds committed online, especially when a number of cards have been hacked online or somehow extracted from a user's history (Warren & Walt, 2007).

2.10.5 Charge Verification System

Charge verification is another effective way to prevent online credit card fraud. It is a process where the seller physically contacts the customer's issuing bank

to validate his or her information (Spann, 2013). I it suggests a physical contact with the person to confirm the details of the card holder (Warren & Walt, 2007).

2.10.6 Cheque Verification System

The cheque verification system is another system that ensures that written cheques are genuine, and whether the account is open and has a reliable cheque history (Warren & Walt, 2007). This system is rarely used, particularly in GCC countries, because the cheque system is not widely used in the region. On the other hand, there is the possibility that such a system could reduce fraud, once the check system has become widespread (Warren & Walt, 2007).

2.10.7 Consumer Authentication System

The system of consumer authentication is widely used to draw the attention of the account holder to an ongoing transaction and seeks the permission to continue with the transaction if it originates from the account holder. The process involves the actual holder of the credit card being authenticated by means of a phone call or email communication (Stamler, Marschdorf & Possamai, 2014). Montague (2011) suggests that it is an effective tool to check whether a person claiming to use a credit card is its actual holder. This is another system devised to combat online fraud commonly used by VISA and MasterCard.

2.10.8 Credit Check System

The credit check system is a system of checking cardholder's identity and credit history of other purchases in the past comparing information given in the fresh purchases with past history (Montague, 2011). The system is widely used by the majority of banks and retail organisations worldwide, and is viewed as

one of the most effective ways to combat real-time and online fraud (Weston, 2009).

2.10.9 Account Ownership Checks System

This account check system helps to check the authenticity of the bank details given by prospective online customer. The account is debited with a pound to see if it goes through or not to confirm the account is for the customer. It has been applied by online-shops and for payment systems (Shavers, 2013).

2.10.10 e-mail Authentication

The email authentication system has also been recently developed and applied to prevent online fraud; it determines the age of the customer, by associating the emails with the demographic data provided by the online users (Singer & Friedman, 2014). It is however doubtful that it can effectively protect against fraud or prevent it, because there are ways in which to misrepresent age or demographic information online in a way that would not allow effective detection (Singer & Friedman, 2014).

2.10.11 Electronic Identity Authentication

The electronic identity authentication system is an updated and more sophisticated version of identity authentication. It involves the collection, authentication and confirmation of the personal identifiable information provided by the online user (Stamler *et al*., 2014). One of the commonly used forms is Know-Your-Customer (KYC) system which helps to gather relevant information electronically about a potential customer to ascertain the true identity and personality of the customer. It is useful in linking the customer to any

involvement of unlawful behaviours in the past for example, in terrorist activities or money laundering.

2.10.12 Out-of-Wallet Checks System

The system of out-of-wallet checks is effective system to prevent fraud. It allows banks or payments systems to physically contact a person and address questions that can only be answered by the genuine owner of the card (Arnold, 2008). It is known under the names “out of pocket” or “knowledge based services” (Montague, 2011).

2.10.13 Reverse Lookup System

The system of reverse lookup is relies on the authenticity of public data held in government records with government agencies. The system includes cross-checking the address and phone information that has been provided by the user through third-party resources in public records (Stamler *et al*., 2014). The system thereby verifies potential customer’s details with records of the customer in the public file or government database (Weber, 2011). Its effectiveness is based on the assumption that public records are unlikely to be forged or otherwise misrepresented.

2.10.14 Return e-mail

The return e-mail system is probably one of the most effective systems in combatting online fraud, but can be associated with certain risks. This system is used mainly to validate a user’s participation in a sale by sending them an email, so that she / he would click on a link or enter a password indicated in the message (Stavroulakis & Stamp, 2010). However, the email of a genuine

customer can be forged or hacked, so that, once the email message is received, it is redirected to the fraudster's address and misuse it (Weber, 2011).

2.10.15 Telephone Number Identification

This is a common method of combatting fraud in online transactions. Using it, payment systems or banks are able to determine the type of telephone that has been used and the company of origin, to verify whether the user is authentic (Montague, 2011). It is probably the most effective method of fraud identification, even though it can also be associated with some risks (Nichols & Lekkas, 2001

2.11 Technological Applications

Technological innovations have made it possible for personal details of the identity and other relevant information of potential customers to be stored and verified online using some technological based forms and platforms. These platforms and devices are now commonly used in banks and other security related transactions. This section reviews some of the devices widely used.

2.11.1 Biometrics

Important and personal unique biometrics of people are now captured and recorded digitally on plastic cards that could be read and verified by special card readers. The information is also stored in central database accessible to any authorised persons anytime. Information about the fingerprints, retinal scans or voiceprints and other personal data such as date of birth, nationality, and Unique National number are captured digitally to be verified digitally as well

anytime (Vacca, 2007). Governments and companies and schools are now using it for passports and identity cards to check frauds. However, it is expensive to implement, and requires some equipment to carry out certain procedures, therefore most retail companies may not be able to implement it (Montague, 2011).

2.11.2 Geo-location

This technology helps to trace and track the location of the customer at the time of transaction. It is usually used to verify the identity of the customer and place of business to satisfy export and other regulatory compliances. The tracing of fraudulent activity by means of geo-location can be considered an effective method, because it can easily detect persons at any location in the world when they are making a purchase (Trost, 2009). It is also effective when a fraudster attempts to hide his or her identity or location, or claims to be in a different place (Montague, 2011).

2.11.3 Digital Signature

Most online transactions now require online agreement in terms of signatures to confirm the terms of transactions. Digital signature is a recent phenomenon, which has become popular in the many business sectors including the banking sector. It is considered the digital equivalent of traditional handwritten signatures (Katz, 2010). Digital signatures are difficult to forge because cryptography is used to deter fraud effectively (Montague, 2011). However, this seemingly secured system remains unclear to many users and has yet to prove its success in many areas (Katz, 2010).

2.11.4 Device Identification

The device identification technique helps to trace and identify the device requesting a transaction to ascertain the authenticity of the transaction. There are different device identification software available to help retail outfit to trace the source of any transaction when there is suspicion of fraudulent practices. Its effectiveness may however be in doubt due to the possibility of deleting and manipulating cookies (Montague, 2011; Long *et al*., 2007; Khanna *et al*., 2006).

2.11.5 Proxy Detection

Proxy detection software is effective means to detect fraudsters operating from anonymous IP addresses (Long *et al*., 2007). However, the problem is, as stated by Montague (2011), it cannot be used directly to detect fraudulent behaviour, even though it may help to determine whether someone is trying to conceal his or her own identity.

2.11.6 Secure Tokens

The secure tokens creating software is yet another way to prevent fraud by authenticating end users (Montague, 2011). However, it is not clear how effective the systems can be in combatting fraud (Mayes & Markantonakis, 2010). Montague (2011) asserts that secure tokens are not effective in detecting the identity of fraudsters and requires an additional task to be done by users. It also needs additional support to validate the unique number (Mayes & Markantonakis, 2010).

2.11.7 Smart Cards

Smart cards are digitally designed and built with stored and regularly updated data that is accessible using card readers installed in retail shops and other offices. There are chips implanted on the cards, which carry the relevant data of the identity of the cardholder. The focus here is however on the card and not the presenter of the card who may not be the real cardholder. The card may not be forged but the presenter of the card may not be real (Mayes & Markantonakis, 2010).

2.11.8 Data Sharing Methods

Data sharing is a rather precautionary method, and mainly serves as an alert for potential fraud, instead of detecting actual fraud. Organisations frequently deploy it; its purpose is to collect and aggregate data from different sources, enabling others to detect fraud (Montague, 2011). The use of data sharing can incur significant expense and may just be used in cases of high risk.

2.12 Counter Measures

The previous sections of this chapter have identified the dramatic increase in online fraud with the advent of technological breakthroughs, which resulted in business losses. Countermeasures to detect and prevent online fraud have become an important aspect of online transactions and businesses. In general, the objective of countermeasures is to stop and prevent online attacks. Countermeasures therefore involve identifying fraud before it happens or as quickly as possible once it has been perpetrated.

Countermeasures therefore are the different measures employed by organisations to identify potential frauds or threats of fraud, to deter potential fraudsters from carrying out the fraud, to put in place infrastructures to prevent fraud, to quickly detect fraud and to punish offenders as deterrent to others. It is noted that an organisation's chances of being defrauded is a function of three variables: the potential fraudster's dishonesty, the opportunity created by the lack of appropriate controls and infrastructures in the organisation, and the motive of the potential fraudster to commit fraud (Yufeng Kou, 2004).

The literature has shown that a mixture of countermeasures aimed at deterring, preventing, detecting and serving punishment or remedy for any fraudulent act is much needed (Moore, 2014). Although there is a need to provide preventive measures to be used as a physical / software hindrance or obstacle, such as secured premises or authentication devices to keep away unauthorised users, it is argued that most preventive measures may impede business functions and negatively affect profit (Moore, 2014). Moreover, recent studies show that even sophisticated preventive measures and techniques are bypassed successfully and frauds are still committed. The focus is now shifting towards actions aimed at remedies, which seek restitution and most importantly to deter others (Spann, 2013; Albrecht *et al*.2011). Research therefore suggests that a combination of countermeasures comprising deterrence activities, preventive activities / techniques, detection activities / techniques and remedy activities could be adopted by organisations for effective control of online fraud (Moore, 2014; O'Hanley & Tiller, 2013).

Previous research has focused on different fraud detection and prevention techniques, but recent events now show the importance of deterring fraud and fraudsters, combining this with prevention techniques, detection and punishment techniques to have a balanced and combined effect on online fraud. This study would thus focus on the examination of the different countermeasures and techniques adopted by the Saudi Arabian financial institutions and government to determine the effect / impact of these countermeasures and the combined effect of the countermeasures on the effective control or prevention of online fraud.

2.13 Summary

The chapter has acknowledged that the penetration of the internet in economies and commerce and the changes brought about in business transactions have provided a platform for the perpetration of online fraud. It highlighted that online fraud is any kind of fraud scheme using any component of the internet for fraudulent solicitations and transactions perpetrated in different disguise, shapes or forms, using the cover of the internet. The chapter also identified different types of online fraud, fraud detection techniques and the countermeasures employed by different organisations to control and prevent online fraud. It also highlighted that the perpetration of fraud depends on many factors, such as the perpetrators' motive, the lack of appropriate controls and the potential fraudster's dishonesty. Countermeasures that consider and take care of all issues that could cause the perpetration of fraud should therefore be collectively employed in organisations.

CHAPTER 3

THEORETICAL APPROACH

3.1 Introduction

This chapter presents the theoretical framework of the research; it examines theoretical bases and theories that could be useful in carrying out an effective examination of the study phenomenon. Some sociological and criminology theories relating to crime prevention and detection will be examined in the chapter, with a view to selecting the most suitable theoretical lens for the current research.

3.2 Criminology Theories and General Detterence Theory (GDT)

The present study focuses on the examination of measures and techniques adopted by Saudi organisations, and how these have effectively controlled or prevented the issues of online fraud in the country. These measures and techniques are regarded as countermeasures, aimed at deterring, preventing, detecting and determining punishment or remedy for any fraudulent act (Kotulic and Clark, 2004).

Countermeasures may be categorised into criminal-centred measures and crime-centred measures, depending on the goal of the countermeasure activities and the techniques used (Beebe and Rao, 2005). Criminal-centred measures focus on addressing the sociological and biological factors that somehow lead to or cause a person to commit a crime and become a criminal.

The concept is based on sociological theories that suggest that there is a societal influence on criminals as they socialise with others with criminal behaviours. Notable theories include social learning theories (Burgess and Akers, 1966) and social bonding theories (Hirschi, 1969). Crime-centred measures focus on addressing the non-sociological factors, but specifically the situation of the crime that reduces the likelihood of the crime being committed. Thus crime-centred measures aim at influencing the criminal's perception of the situation of the crime as being too risky and of no benefit, and therefore attempt to forestall the crime from occurring in the first instance (Clarke, 1980).

Computer security theories are based on three main explanations that reflect the main perspectives of computer crimes. The first explanation argues that potential criminal offenders, who are greatly influenced by their perceptions of the net benefits associated with committing the crime, could be deterred by the certainty and severity of punishment (Straub, 1987, 1990). The second explanation argues that computer criminals commit crimes according to the motivation they derive from goals and intentions. Thus an understanding of the motivation of computer criminals could help prevent computer crime (Smith and Rupp, 2002; Denning, 1998; Chantler, 1996). The third explanation suggests that the effectiveness of information system countermeasures may be a function of the balanced implementation of technical, formal and informal controls (Dhillon *et al*., 2004).

Most computer security theories focus on environmental and physical security, while GDT focus on countermeasure activities and relationships, and their

collective effect on online fraud. For example, the situational crime prevention theory addresses the physical crime situation and examines how the crime situation reduces opportunities for potential criminals. The theory recognises many opportunity-reducing techniques, which are classified into four categories that have a direct impact on potential criminals' decision-making processes. The first category relates to the increased perceived level of the effort to commit the crime, while the second category relates to the increased perceived risk of being caught; the third category attempts to reduce the criminal's anticipated rewards, while the fourth category attempts to remove the potential criminal's excuse (Clarke, 1997).

Some criminological theories used in the examination of crimes and criminal activities have in most cases critically examined the criminals' motivation and the authority in place (Foucault, 1977: Cornish and Clarke, 1986), while some theories considered social environment influencing the crime (Hirschi 1969; Bursik 1988).

Some criminological theories used in the examination of crimes and criminal activities focus on the power of authority (Foucault, 1977) or the motivations of criminals (Cornish and Clarke, 1986), while some theories focus on the influence of social conditions and environment on crime (Hirschi 1969; Bursik 1988).

3.2.1 Social Disorganisation Theory

Another notable social theory of crime is the social disorganisation theory, which argues that crime occurs when communities are weak and disorganised as a result of economic disadvantage and residential instability. The residential instability of communities is, in most cases, a result of the movement of people

to and from a city or community, which creates mixed culture, behaviour, educational and technological backgrounds, as well as economic power and motivation. This mixture causes instability and disorganisation in the community, which may negatively affect it. The theory therefore argues that, as communities become more developed and organised socially - having clearly defined collective moral ethics and codes of conduct with respect to community values - and economically, their ability and influence on crime increases and make crime deterrence more effective. It is therefore appropriate to examine the effects of community on crime (Bursik 1988; Kubrin and Weitzer 2003; Triplett et al., 2003).

The social disorganisation theory focuses on the influence of social conditions, as based on the development of the community. It is assumed that developments in economic and social conditions (culture, respect, trust, bonding and family ties) can determine the norms and codes of behaviour in the neighbourhood, and may have an effect crime rates in the community. It is noted that the prevailing residential culture in an area may influence or make the residents more wary about criminal activity. The resident culture developed over a period therefore impacts on the behavioural attitude of the residents, and has an impact on criminal activity (Anderson 1999; Sampson et al., 2002; Triplett et al., 2003). The social disorganisation theory also highlights the issue and influence of respect in communities. It posits that respect is earned in a community, which affects criminality in the area (Bourgois, 1996). Socially acceptable and unacceptable norms and codes of living in the area are clearly defined and approved by community leaders, according to accepted community values and cultural heritage (Brewer et al., 1998). This forms the bases of the

informal social controls that communities apply to reduce crime. It is noted that, in many cases, community regulation based on community codes of conduct produces high quality results than regulation by formal authorities, such as the police (Bennett, 1995). Research shows that neighbourhood watch programmes organised and managed by government departments, work less effectively than those organised by community leaders (Bennett, 1995). Therefore, the social disorganisation theory focuses on the communal regulation of criminal activity and the relationships of the community with the authorities in efforts to combat crime. The theory suggests that in the absence of strong authority-based control, there is the likelihood of the formation of communities or vigilante groups in the community to fight crime on its own. However, communities may apply some form of informal social controls to reduce crime, but the effectiveness may depend on the community members' degree of attachment to their neighbours and their physical locality (Silver and Miller, 2004).

This is based on the social relationships the members have with their community - the respect that members have for the culture of the community and how they have been integrated into the community. The theory thus suggests that a member who is permanently resident and fully integrated in the community is likely to join hands with other likeminded people in the community to stop the increase of crime in order to preserve the safety and quality of the environment (Adler and Kwon, 2002). Anticrime communities are more likely to form when a substantial proportion of individuals make up their minds to permanently reside within a community, but when most people entering the community are mere passing by on a journey, it is unlikely that any anticrime

communities would form (Taylor, 1996).

Social disorganisation theory focuses primarily on the attachment of community members to the physical neighbourhood, and how this attachment forms anticrime communities to regulate crime in the area (Sampson and Groves, 1989).

It describes neighbourhood attachment as an important element in informal social controls - the formation of anticrime communities and the regulation of crimes in an environment. Neighbourhood attachment is seen as a major motivation for community responses to crime. The theory is thus useful in examining the role of the community in regulating fraud and crime. The theory also shows the importance of the development of informal (clan) social controls, distinct from the formal (authority- based) controls that have failed many communities in crime prevention. More often than not, the informal (clan) social controls established in communities are as a result of dissatisfaction with the authority and formal (authority-based) controls on how crime is managed in the community (Nolan et al., 2004). Most communities thus have developed to the extent of influencing their members by associating in informal, social relationships and trust (Adler, 2001). Unlike a large majority of criminological theories that mainly considers the power of authority (Foucault, 1977) or criminals' intents and factors that influences his actions (Cornish and Clarke, 1986), which focus on the individual at individual level, the social disorganisation theory focuses on the influence of social conditions on crime and therefore focuses directly on the community and how the community, through its informal clan-based controls, regulates crime in the area. Research in criminology, however, stated that an emphasis on personal preferences does

not give a better understanding of criminal activity, as it avoids the social influences of crime and the context the crimes are committed with its evidential consequences, thus making the choice of the social disorganisation theory an attractive theory for this research. However, the focus of this research is on the examination of the countermeasures and techniques adopted by Saudi banks and financial institutions aimed at deterring, preventing, detecting and according punishment or remedy for any fraudulent act. Although both the technological and social cultural countermeasures may be examined, the social disorganisation theory may not be suitable for this research, as it concentrates on the actions of community leaders and community regulations.

Another main reason why the social disorganisation theory may not be suitable is that the theory also focuses on how communities are developed to set up norms to fight crime within the community in association with other established legal authorities. The present study does not focus on how Saudi Arabian communities develop their relationship with law enforcement agencies. Aspects of the theory may however be used in the examination of the influence of the social environment on the rate and prevalence of online fraud in Saudi Arabia.

3.2.2 General Deterrence Theory

For the purposes of the present study, it seems that the most appropriate and suitable theory to help in the investigation is the General Deterrence Theory (GDT). GDT is based on the argument that individuals who commit crimes may be dissuaded from pursuing such crimes through the use of countermeasures (Straub and Welke, 1998). GDT has been applied to the study of information systems security efficiency in different dimensions. One key dimension is the examination of information security actions and how the interactions of the

managers and those that commit the crime affect their security actions (Nance and Straub, 1988). GDT suggest that information security actions may deter potential criminals from carrying out unlawful acts against organisational policies. The theory has also empirically proved that actions based on security threats can reduce systems risk. The importance of the activities of managers in the successful deterrence, prevention and detection of fraud and in the punishment of offenders has also been noted (Straub and Welke, 1998).

It views deterrence as influencing decision-making, which may require altering or reinforcing how decision- makers perceive the key factors that need to be considered before they act (Kelvin Cgilton, 2009). Moreover, GDT is an appropriate proactive theory in the attempt to prevent crime before it is committed, suggesting that using deterrence, prevention, detection and remedy countermeasures could mitigate threats of fraud. As the present study focuses on online prevention, the theory allows for a systematic approach to combating fraud, by creating an environment or situation that deters the commitment of fraud and emplacing measures to prevent fraud from occurring, while, if it occurs, to systematically detect the fraud with purposeful detection activities

3.3 Fraud theories and GDT

Several fraud theories have been propounded by different researchers to understand crimes, criminals and situations surrounding fraud. Such theories and studies include Sutherland's 1939 "white-collar crimes and the theory of differential association which opines that crime is learned, not genetic and learned from intimate personal groups''. Another significant fraud theory is Cressey's 1950 fraud triangle which classifies offenders and why they commit

fraud and violate trust. The fraud triangle identifies three main factors that may affect the criminal behaviours of the offenders, namely pressure that drives the need of the offender, opportunities enhanced by lack of appropriate controls and access to information and rationalisation of reasons to commit the crime. Controlling crime therefore may require the proper management of these factors. Another related and significant fraud theory is the Albrecht's fraud scale which opines that strong situational pressures and high perceived opportunities due to poor controls, and low personal integrity due to the individual code of behaviour, will contribute to a high tendency of committing crime, or will scale high in the fraud scale.

However, Hollinger and Clark 1983 study highlights the importance of organisational controls and policy developments in the control of fraud and criminal activities in an organisation. The study opines that company policies, the staff selection, inventory control, security and punishments are instrumental to the control of fraud. The theory postulates that there are four key aspects of policy development that are essential in controlling fraud namely, the understanding of theft behaviour, the spreading of positive information on company's policies, the enforcement of sanctions and publicising sanctions. The theory aims to affect the behaviour of the criminal by countering the criminal's justification of the crime, morally, legally and through consequences.

It also posits that organisations need to hire the right people as staff, and have reasonable expectations of them. The theory therefore argues that for effective management and control of fraud, the criminal's intention and behaviour need

to be influenced through the use of organisational controls and policies targeted at the criminal's perception for deterrence and the establishment of controls to deter, prevent and detect fraudulent activities.

Most studies have however focused on crimes, the criminals or both as opposed to the methods, procedures and organisational policies. Wilhelm (2004) therefore proposes that the control of fraud requires a comprehensive fraud management lifecycle of stages comprising deterrence, prevention, detection, mitigation, analysis, policy, investigation, and prosecution.

This implies that effective control and management of fraud requires a balancing of the competing and complementary components and processes within the fraud management lifecycle. The fraud management lifecycle theory posits that there are different stages in the lifecycle of fraud management which interact with each other and complement each other for a successful management and control of fraud in organisations. Failure to successfully balance the focus on the various stages or components of the lifecycle, and failure to successfully integrate the stages and use appropriate technologies in the stages, may result in poor control of fraud in organisations. The Fraud Management Lifecycle is, therefore implied to be a network lifecycle with each stage/node in the network/lifecycle is seen as an aggregated entity that is made up of interrelated, interdependent, and independent actions, functions, and operations (Wilhelm, 2004).

The General Deterrence Theory (GDT) corroborates the fraud management lifecycle theory and is thus opined to have four interlinking components to effectively control and manage fraud, namely deterrence, prevention, detection and remedy. It proposes that the successful balancing of activities within and between these main components will enhance effective fraud management and control. Deterrence is defined as the inhibition of criminal behaviour through fear of punishment. It is characterized by actions and activities aimed at stopping fraud before it is attempted which may result into turning aside or discouraging even the attempt at fraud (Wilhelm, 2004). Deterrence activities are regarded as passive, as there is no inherent mechanism for ensuring enforcement, thereby relying on the individual for compliance. It is also noted that the aggregate nature of deterrence is implied; it is also an aggregation of activities with varying degrees of deterrent value and cannot be viewed as a monolithic whole.

The aim of deterrence is thus to provide disincentives for potential computer fraudsters (Whitman, 2004). However the limitation of deterrence activities or measures necessitates the prevention of fraud. However, GDTs argue the need to provide preventive measures to be used as a physical / software hindrance or obstacle, such as secured premises or authentication devices to thwart unauthorised users. Although most Information systems have focused on this aspect to avoid the disruption and damage caused by fraudulent acts, they have been successful to some extent. On the other hand, it is also argued that most preventive measures may impede business functions and negatively affect profit (Gopal and Sanders, 1997). Moreover, recent studies show that

even sophisticated preventive measures and techniques are successfully bypassed, and frauds are still committed. The success of the deterrence component is therefore contingent upon the performance of the other components; hence the need for measures and techniques to detect fraud is therefore sustained by GDT.

Preventive activities are closely associated with deterrence and detection but are usually noticed after the obvious failure of deterrence and before the suspicion or detection of fraud has been accomplished. Prevention activities are therefore aimed to hinder, check, or stop a fraudster from performing or perpetrating a fraudulent activity. The activities are meant to harden the fraud target .

Detection activities on the other hand are targeted at identifying and locating fraud prior to, during, and subsequent to the completion of the fraudulent activity. Detection is therefore defined as the process of attempting to discover security breaches within a system, either through internal system controls or purposeful detection activities. Thus, detection activities include actions and steps to reveal the existence of fraud testing and fraud attempts, as well as successful frauds.

Furthermore, when fraud is detected, or even in the absence of fraud, GDTs suggest the need for a legal order to prevent or redress a wrong or enforcing right. Actions geared towards remedies therefore serve to seek restitution and most importantly to deter others (Cheng *et al*., 1997).

GDTs suggest that the activities of the four components mostly serve to deter and prevent fraud. The measures and techniques adopted in Saudi Arabia in

terms of regulations, technology and awareness are examined to determine how they have been able to deter, prevent, detect and remedy fraud in Saudi Arabia.

3.4 Theoretical Framework / Model – General Deterrence Theory (GDT)

The theoretical framework of this research will be based on the provisions and components of general deterrence theory (GDT). GDT is the proactive use of deterrence, prevention, detection and remedy to prevent crime before it is committed (see fig 1). Its provisions and components will be useful in the investigation of the subject matter in this research. The theory therefore allows for a systematic approach to combating fraud, first by creating an environment or situation that deters people from committing fraud, and emplace measures to prevent fraud from occurring, but, if it occurs, to systematically detect the fraud with purposeful detection activities, and reprimand offenders.

The study is aimed at investigating how financial institutions using countermeasures employ a systematic approach to enhance the effectiveness of the countermeasures.The theory posits that the different components or groups of activities namely deterrence, prevention, detection and remedy are important with different values and benefits to add to the successful control and management of fraud. The components interact with each other and complement each other for a successful management and control of fraud in organisations. The theory therefore calls for a proper management of the interactions and a balancing of the focus on each of the components which are equally important to the overall success of fraud control and management.

All the components work together to stop fraud; the activities in each component and the relationships between the components become very important in the success of the approach / theory. The theory therefore argues that the success of any effort or approach to combat fraudulent activities depends on the activities of these four components, which must be visibly seen to be in operation in organisations. Some organisations may focus on only one or two of the components, such as prevention and detection, while silent on the others.

The theory also suggests that there should be a systematic approach to the organisation and coordination of the interrelated components. For example, remedy is at the centre of the systematic approach. It serves as a corrective and punitive measure for detected crime, aimed at deterring potential criminals. This implies that, without detection of crime, punitive measures cannot be applied to deter others. Deterrence activities such as awareness creation and the training of staff may also enhance better prevention of crimes, as people become more vigilant. A high detection rate may also mean that the preventive and deterrence measures have failed. This shows the relationships between the components and the importance of the components working systematically together. The framework / module of this research based on the GDT therefore examines the activities of each component of deterrence, prevention, detection and remedy, their individual and collective relationships and their overall impact on preventing online fraud. The composition of the components, their activities and the interrelationships between the components will be studied as part of the research framework. Deterrence, prevention, detection and remedy

activities in the study organisations will therefore be examined, to determine how they are systematically organised to stop fraud in Saudi Arabia.

The framework proposes that deterrence activities are supposed to create awareness and inhibit fraud, with the intent of stopping crimes before they are carried out. Deterrence activities also help facilitate prevention activities by establishing necessary awareness for the operators of the system. Prevention activities also work to enhance detection activities, and remedy activities help in deterring others. The model therefore suggests that prevention, detection and remedy are all encapsulated in deterrence, all working together to deter and stop online fraud. The framework as discussed will therefore be used to carry out the investigation, the data collection and analysis, and interpretation of results. Figure 1 shows the GDT components, their relationships and Interdependencies.

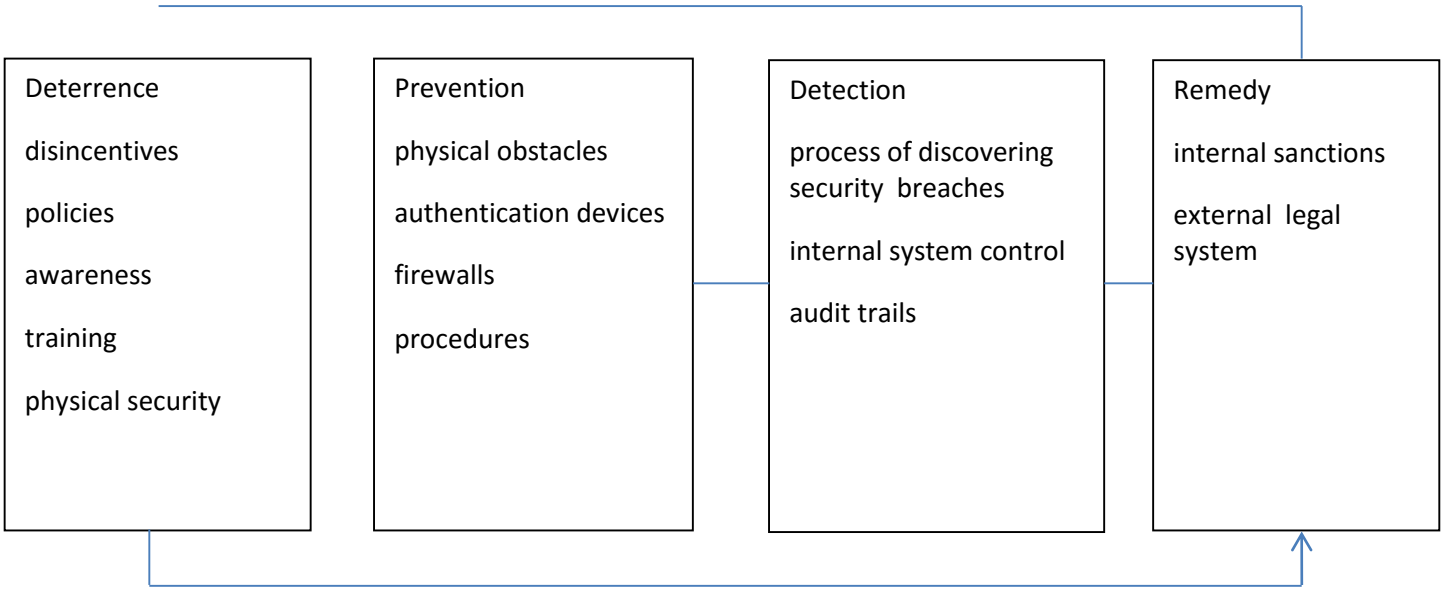


Figure1 GDT components

3.4 Summary

This chapter examined some of the theoretical bases of countermeasures, namely criminal-centred measures and crime-centred measures. The chapter concludes that crime-centred measures focus on addressing the non-sociological factors, but specifically the situation of the crime that reduces the likelihood of the crime being committed, and makes it suitable for the present research aims and objectives. The choice is made to use the GDT framework, which aims at influencing the criminals' perceptions of the situation of the crime as being too risky and of no benefit; it therefore attempts to forestall the crime from occurring in the first instance. One notable benefit of the GDT chosen is the key dimension of the examination of information security actions and the underlying relationship between the activities of managers and of computer abusers, which is critical in lowering systems risk, the successful deterrence, prevention and detection of fraud and in the punishment of offenders (Nance and Straub, 1988; Straub and Welke, 1998; Beebe and Rao, 2005).

CHAPTER 4

RESEARCH METHODOLOGY

4.1 Introduction

Chapter 3 concluded with the development of a theoretical framework to guide the research investigation. The framework, which is based on general deterrence theory, highlighted the four main components of the research, which constitute the focus of research. The components are deterrence, prevention, detection and remedy activities, which were examined individually, and collectively to determine how they are systematically organised and their overall effect as regards stopping online fraud in Saudi Arabia. The theoretical framework thus identifies the focus of research and how the investigation needs to be carried out to provide answers to the research question on how countermeasures can have an impact on online fraud. This was useful in this chapter in determining the choice of a suitable research approach for this study.

A research approach defines the processes of investigation and how the required knowledge of the subject matter may be acquired. This will be based on how the nature of reality is perceived (ontology) and how the nature of knowledge claims can be obtained (epistemology). Thus, there are different possible approaches in any research investigation. A research approach therefore defines justifiable action plans to lead to a successful research investigation. This chapter considered the processes of investigation and

justified the choice of the research approach suitable for the study. The choice of a research approach is based on the ontological and epistemological assumptions that determine how the required knowledge of the subject matter may be acquired and how the nature of knowledge claims can be obtained. Meanwhile, these assumptions may also depend on the nature / type of study and objectives / motives of research.

4.2 Research Motivation

It is pertinent to note that every piece of research has a major aim that drives and guides the investigation of the subject matter. Research motivation therefore plays an important role in research methodology, as it facilitates the choice of appropriate and suitable methods for the particular type of research that will guarantee the completeness and objectivity of the research (Flick, 2011). The general concept of research, which is a systematized effort to gain new knowledge, centres on the notion of manipulation, based on the motivation or objectives for the research (Kothar, 1990). In the context of social research it is a concept which is manipulated by the notion of knowledge (Creswell, 2008).

There are certain objectives for research, but the most common objectives are (i) gaining familiarity with a certain phenomenon or getting new insights into the phenomenon; (ii) accurately portraying the characteristics (iii) determination of the frequency with which something occurs or with which it is associated with something else; (iv) testing a hypothesis of a causal relationship between variables (Kothar, 2004).

Kothar (2004) identifies each of these objectives with certain fields of research studies: (i) exploratory or formulative research studies; (ii) descriptive research studies; (iii) diagnostic research studies and (iv) hypothesis-testing research studies. The research objective of this study is focused on exploring online fraud in Saudi Arabia and the impact of countermeasures. The systematization of research objectives is necessary, since it helps the researcher to understand which direction or approach should be taken in the course of study. Nonetheless, an important aspect of research is research motivation. Kothar (2004) identifies the following motivational aspects (fig 2), which are the desires of research rather than motivation:

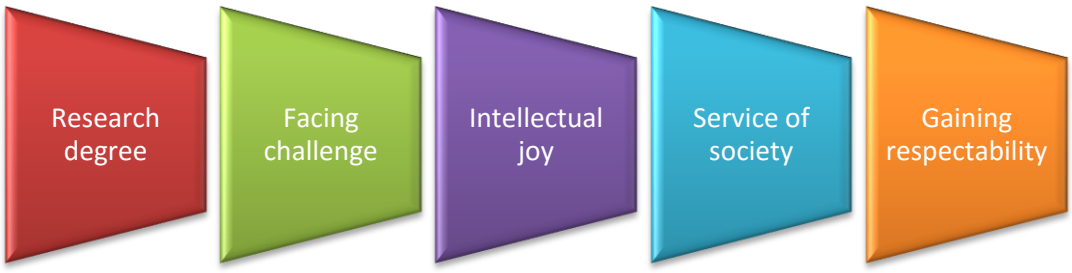


Figure 2 Research Motivations

These factors are pivotal in determining, not only the course of research, but also in making research more effective. Kothar (2004), believes that the list of objectives are not meant to be exhaustive, because there can be as many motivations as possible, which cannot be subject to certain calculations or systematization. The motivation for this research may be primarily based on exploring the countermeasures of online fraud in Saudi Arabia in fulfilling the requirement for the award of a degree, but the research will also bring intellectual joy to the researcher and be of service to the society.

4.3 Nature of Research

Certain types of research may require specific research methods. Areas such as social research, because of its particular study requirements, will need a certain approach .The aim of the study will also direct the type of approach required for study and the research strategy.

Online fraud is a social issue that is usually shrouded in secrecy and embedded in societal norms. This is coupled with the selected country of focus, Saudi Arabia being my country known for religious standards and faith in Islam. The examination of the countermeasures adopted by the banks in Saudi Arabia makes the study more interesting and requires inquiry, explorations and revelations in greater depth. The study therefore focuses on the tech socio-technical and not pure technological phenomena surrounding or influencing online fraud within its 'real life' context.

This study focus thus highlights the peculiar nature and complexity of the subject matter of which relatively little is known, thus making the research exploratory in nature. The nature of this research and the type of research question therefore suggests the choice of a research approach that would enable better interpretation of the basic characteristics of the social phenomenon of online fraud in Saudi Arabia, for a more complete understanding of the socio-technical context of the countermeasures of online fraud.

It should be noted that, because the issue of online fraud is exploratory (a social issue that requires in-depth inquiry in its real life context), the reality might be dependent on the researcher and the interpretation of the participants. This may therefore be based on the ontological assumption of subjective idealism (Archer, 1988). Moreover, the required knowledge may be ideological and based on the social context of study, which suggests a epistemological assumption. However, because the exploratory nature of study also requires facts and not just values to be established, positivism epistemological assumption which ‘’believes that facts and values are distinct and scientific knowledge consists only of facts ‘’may also be considered in the process of this research.(Archer,1988).

Dawson (2009) therefore describes research methodology as “the philosophy or the general principle which will guide research” (p. 15), and are about tools used to gather data which are based on some philosophical assumptions.

It is therefore important first to define the research philosophy which forms the basis of research methodology and then attempt to highlight research methods to be applied in the context of the present research. It should also be noted that the outcomes and effectiveness of study depends on the research methodology.

4.4 Research Methodology

Research methodology defines action plans and the designs of how the required knowledge of the research focus as defined in the research question and aims can be acquired effectively to meet the objectives of the research and

answer the research question (Yin, 2002). The chosen methodology will however depend on the ontological and epistemological assumptions and the chosen research philosophy, either positivism or interprevitism. This implies that there are different types of research approach that may be suitable for different types of research, as determined by their objectives. Study may also be chosen according to a philosophical view of both the objective and how this objective knowledge may be gained. (Hennink *et al*., 2011 Myers 2009).

4.4.1 Research Philosophy

One of the main elements that underline research methodology is research philosophy. Research philosophy, is concerned with certain beliefs that touch upon the ways in which the data for research should be gathered, analysed and applied (Bridges & Smith, 2007). The beliefs concern the nature of reality and how knowledge can be obtained. Research philosophy therefore depends on some ontological (reality) and epistemological (knowledge) assumptions.

4.4.1.1 Ontology

Ontology concerns the nature of reality, which has been classified in three ways: external realism, internal realism and subjective idealism. External realism is concerned about the existence of reality independent the of researcher's interpretation. Subjective idealism argues that construction of reality is dependent on the researcher, as each researcher interprets the situation subjectively, while internal realism stands in the middle between external realism and subjective idealism, seeing the existence of reality independent of the interpretation of the researcher but at the same time seeing that more of the reality can be revealed by the researcher's construction of the

situation (Archer, 1988). The classification is like a continuum of two extremes: the external realism and subjective idealism which underlie the two distinguished research approaches positivism (quantitative) and interpretive (qualitative). While external realism believes that there is an existing truth that must be discovered, not necessarily be by the researcher's formulation of the truth, the subjective idealism believes that the truth may only be generated through the research formulation of the researcher. Meanwhile the internal realism view, which is a middle-of-the road stand, lends itself to a mixed method approach accommodating the benefits of the two views.

4.4.1.2 Epistemology

Epistemology relates to the definition of ''knowledge and how it may be obtained'' (Myers 1997). It is also classified in three ways, namely positivism which is based on the assumption of the distinction between facts and values and that scientific knowledge consists only of facts; non-positivism which is based on the assumption that facts and values are intertwined in scientific knowledge and are difficult to separate; and normativism which views scientific knowledge as being ideological requiring examination of the experiences of the participants and their values (Archer, 1988).

This classification also supports the two main research methodological approaches namely quantitative methodology which focuses and aims at the facts obtainable in the field; and qualitative methodology which acknowledges the facts in the field but also considers the importance of the values and the meaning of knowledge as described by participants from their experiences.

4.5 Research Approaches

There are two main types of research approaches namely qualitative and quantitative research, which have different underlying assumptions. The distinctions between the approaches are based on their underlying assumptions which include their ontological assumption on the objectiveness or subjectiveness of the nature of reality; and their epistemological assumption of general focus of what can be obtained or specific focus on only facts and ignoring values. Moreover, the distinction may also be based on the nature of study whether focused on prediction of the future or simply exploratory and giving explanations (Hennink *et al,* 2011; Bryman 2001; Myers 2009).

Based on some ontological (reality) and epistemological (knowledge) assumptions, most research takes either of the two main philosophical positions (positivist and interpretivist) (Collis and Hussey, 2003). However, the classification of research methodology into two major classes represents different ends on a continuum rather than polar opposites.

The researcher may choose to take the strongest elements of each methodological approach in combination (Newman and Benz, 1998. This makes it possible for the researcher to obtain the optimum of the two methodologies for a fuller comprehension of the subject matte (Creswell and Plano Clark, 2007).

The study of online fraud in Saudi Arabia may require an objective study focusing on the facts, but, at the same time, may rely on the subjective

experiences of the parties involved in the online fraud, to gain a deeper understanding of the phenomenon.

4.5.1 Qualitative Research

Qualitative research is usually designed to “help understand people and the social and cultural contexts within which they live” (Myers, 2009). This allows for the research to learn from the experiences of the participants and get the insiders’ views of the study matter. This makes qualitative methodological approach suitable for the study of socio-cultural issues which requires the use of the natural settings of the study in getting natural data. Quantitative research on the other hand may be more suitable for the study of natural sciences which requires fact-based data. Moreover, the natural settings and the data collection techniques of qualitative research makes it possible to obtain both facts and values attached to the issues and thereby explore the meanings of issues raised and give a better understanding from the perspective of the insider (Bryman, 2001;; Creswell, 2007 Myers, 2009).

Qualitative research also allows data collection methods that are flexible, open and comfortable with the participants that allow them to give both facts and values or interpretation of issues which can be captured, in its natural meanings and in their own words (Sarantakos, 2005; Kaplan and Maxwell, 1994). This increases the quality and richness of the qualitative data collected and enables detailed interpretation and construction of the reality of the subject matter.

4.5.1.1 The Interpretive / Realist Philosophy in Qualitative Research

Interpretive research adopts the subjective idealism philosophical view; with the assumption that truth or the reality of the subject matter may be best obtained based on the researcher's construction of the situation. Interpretive research is therefore based on the construction or the interpretation of the personal experience of the participant and the researcher, which may be based on some personal ideology. Its ontological stand is thereby subjective and interpretive. The epistemological stand of interpretive research is also based on normativism, which views scientific knowledge as being ideological, implying that knowledge may only be obtained by looking deeply into the values attached to the experiences of the participants.

4.5.2 Quantitative Research

Quantitative research is designed to adopt an objective approach of obtaining required data in an investigation. The approach therefore ensures that only required facts are obtained through quantification of the data which becomes measurable and subject to scientific principles. Quantitative approach is therefore more suitable examine cause effect relationships of variables in natural sciences. The approach is therefore associated with statistical analysis for inferential and descriptive reports of study phenomenon (Bryman, 2001). It therefore relies on a process of statistical instruments to measure and test objective theories and hypotheses (Bryman, 2001). Quantitative research strength is in providing accurate objective picture of the data but lacks certain flexibility of interpretation. However, due to the focus of quantitative

approach on only facts, it is argued that the approach captures only still pictures and not details or meanings behind the given facts. its data collection methods are also often closed methods which limits required answers to “Yes or No; 1 or 2” (Sarantakos, 2005).

4.5.2.1 The Positivist Philosophy of Quantitative Research

Positivist theory emphasises the necessity for objective observation and description of phenomena, ignoring comprehensive analysis (Prasad, 2005). This is because positivists strongly believe that phenomena can be studied in isolation, without further inquiry into details (Prasad, 2005). Therefore, positivist philosophy underpins most modern scientific research.

The positivist philosophical position is based on an external, realist, ontological stand, ‘’which considers reality as existing independently of the researcher’s construction of it ‘’ (Archer, 1988). It relies on the view of the social world as comprised of facts, items and objects and thus adopts a deductive and objectivist approach. It is therefore more suitable and mostly used for the study of natural phenomena, which often requires the measurement of the relationships among variables. This enhances the deductive testing of objective theories in the form of hypotheses, and at the same time determines the cause-effect relationships between the study variables (Bryman 2001).

One of the main tenets of positivist theory is that it allows researchers to manipulate reality with different variants of a single variable and to make conclusions on what has been observed or explained so far (Prasad, 2005). It is also argued that the positivist philosophical position takes the researcher

away from reality which can be better captured and understood from the inside, but only allows the capture of still pictures of the reality (Sarantakos, 2005; Hennink *et al.*, 2011).

4.6 Research Strategies

Research strategy is important as it determines the course of the whole research process and the activities required to conduct the research investigation. There are different strategies designed and used for different purposes (Costanzo & MacKay, 2010). For example field experiments are widely used in social research, particularly in the context of organisations (Harrison, 2004). Surveys are major tools that are used for field experiments, but field experiments are not only confined to surveys (Harrison, 2004).

One of the disadvantages of a field experiment is that it may provide a researcher with biased and subjective information in terms of subject matter; therefore researchers are often cautious about the results of such a study by pointing to the narrowness of their field study (Harrison, 2004). On the other hand, they circumscribe this problem by critically comparing it to theoretical sources, such as academic books, articles and conference papers as well as statistical reports (Harrison, 2004).

In terms of the present research, case study is the most appropriate and relevant research strategy, as the study is focused on a specific study phenomenon in a selected sample population for a detailed study and generalisation. The research focus of this study is the examination of online

fraud and the effectiveness of the countermeasures which may require a case study of the financial organisations in Saudi Arabia and how they have effectively addressed the issues of online fraud. The conclusions of this report may therefore be used in other areas both in the Saudi Arabia and other countries. The case study strategy may be effectively carried out using tools such as interviews and observation of bank processes to obtain relevant data on online fraud and the effectiveness of the countermeasures adopted.

The study of Ahmed, Buragga and Ramani (2011), confirms the usefulness of case study as it helped in successfully identifying the security issues that exist in e-learning in Saudi Arabia. Moreover, the study also summarized the main concerns for e-learning in Saudi Arabia, as follows: (i) user authorization and authentication; (ii) entry points; (iii) dynamic nature; (iv) protection against manipulation; (v) confidentiality; (vi) integrity; (vii) availability; and (viii) non-repudiation (p. 1,580).

It is useful to acknowledge a comprehensive study conducted by Shalhoub (2006), who surveyed the privacy policies of 183 websites in GCC countries. It is a good example of analysis of organisational documents. His study not only embraced specific industries, but extended to several areas, such as accommodation and food services, waste management and remediation services, agriculture, forestry and others. That study was carried out with the intention of determining: (1) the number of GCC companies that had privacy policies on their websites; (2) whether privacy policies are different according to industry type; (3) the content of the online privacy policy statements; and (4)

the extent to which the websites addressed each of the five FTP dimensions. The above criteria were designed to establish the boundaries of examination in organisational documents, through which effective research is determined.

4.7 Selected Research Approach

A qualitative research method was chosen for the investigation. The approach is designed to help in the exploratory investigation, using a wider population, leading to effective analysis. The qualitative approach was also used for in-depth investigation using a thematic method to identify issues of concern from the data sets collected, while highlighting sub-themes and themes.

4.8 Research Design

Hennink *et al*. (2011) suggest that a research design is a framework of strategies or methods of inquiry uniquely designed to fit the nature of the research, and guide the conduct of the investigation. It sets out plans and processes for the collection and analysis of the required data in different forms and formats. Different strategies of inquiry using associated tools or techniques for effective data collection and analysis can be employed to set up an appropriate research design for effective conduct of the research. Possible strategies or methods of inquiries include case study, experiments, field surveys etc. (Markus and Robey, 1998; Myers, 2009; Hennink *et al*., 2011)

Based on the choice of research approach, the research method of inquiry is the interpretative case study method, which allows for deep insight into situations, and enables a deeper investigation of contemporary phenomena,

such as online fraudulent practices within real life contexts. It is to be noted that a case study is more suitable in this situation, ‘‘especially when the boundaries between phenomena and context are not evident’’ (Yin, 2003, p13). The researcher, as an independent observer, can also easily highlight issues in the environment and examine phenomena in their natural setting. Mingers (2001) explains that the investigation of complex social and organisational issues requires deep understanding, which can best be achieved using an in-depth case study method, described as a capable and effective vehicle for interpretative investigations (Mingers, 2001). The case study method allows for the collection of past historical data, present life actions and future expectations, thereby putting issues in their social and historical context, to give an understanding of the emergence of the current situation (Montealegre, 1999; Klein and Myers, 1999).

4.8.1 Case Study Design

The focus of the research is the examination of the impact of organisational countermeasures on the deterrence, prevention, detection and remedy of online fraud in Saudi Banks and financial institutions in Saudi Arabia, and supervising / regulatory departments are therefore chosen as appropriate case study organisations. The case study was thus designed as a single case where the issues identified in the research framework will be holistically represented. The design will also allow the interactions between the various countermeasures, the influences of organisational practices and the environment on the impact of the countermeasures to be explored in-depth.

The focus of the research and the framework also helped to determine the selection of participants for the research. For the investigation of countermeasures, the banks and regulating ministries / departments were involved, while, for the investigation of the perceptions and environmental impacts, bank customers and the government took part. The staff of the concerned banks and ministries / departments were selected to partake in the investigation, which was carried out using interviews.

Therefore, for better understanding of these issues, the experiences of bank staff and other financial institutions would be required. The focus of investigation and the participants in the study will be bank staff who are able to give relevant data and information required. However, some customers who have been victims of online fraud may have to be involved to give their opinion to add another perception.

4.8.2 Case Study of Saudi Banking Sector

The prudent financial system regulation of the Saudi Arabian government has been described as a major strength of the economy. The government has maintained macroeconomic stability through continued strong financial supervision and fiscal reforms. Policies have been designed to promote financial development while maintaining large fiscal buffers. High government spending and increase in public spending also contributed to the high liquidity of the banks which has boosted the banks intermediation role in the economy. The high deposits in Saudi banks have continued to be the main source of funding and activity driver accounting for three quarter of the total balance sheet as at March ending of 2014.(, International Monetary Fund, 2012).

The need to strengthen the financial regulatory framework led to the setting up of the Saudi Arabian Monetary Agency (SAMA) with primary responsibility for monetary policy in 1952. With increased power and renewed mandate in 1990s, SAMA took steps through policies to encourage banks improve their risk management and control procedures through the setting up of internal audit / risk management departments and the implementation of internal controls. Main objective of the policies and regulatory initiatives was to create a suitable infrastructure for effective monitoring that required sound corporate governance of banks. Banks were required by the new initiatives to meet stringent conditions for capital adequacy, liquidity, and lending ratio and reserve requirements. Furthermore, the issues of banks expanding too rapidly and uncontrollably were checked and monitored while ensuring that banks have adequate credit assessment and monitoring procedures, required technical expertise, required qualified human resources and adequate technology. Most banks however lacked the required expertise to understand and manage the control of fraud. The awareness of the state of online fraud was also lacking with most bank officials. (International Monetary Fund, 2012).

Although the legal framework based on the 1966 SAMA act/law is old, SAMA has been able to take adequate actions without using formal legal powers. SAMA has also made substantial efforts to introduce Basel II aimed at ensuring effective risk management and maintain growth.

Thus the banking sector in Saudi has maintained significant growth rate in assets and credits above that of the GCC banking sector in 2011 and thus is regarded as the most expansive banking market in the Gulf council cooperation (GCC) (Algamdi, 2012; Gulf base, 2013). It has been noted that the growth of

public expenditure by the Saudi Arabia government affects corporate loan demand and retail credit growth, which has had notable impact on the structure, and growth of the banking sector in Saudi Arabia. Assertive government regulation and over generous public spending have therefore strengthened Saudi Arabian‘s banking sector (Algamdi, 2012; Gulf base, 2013). There are twelve main banks operating in Saudi, the banks with their net assets and net income are listed below (Figure 3).

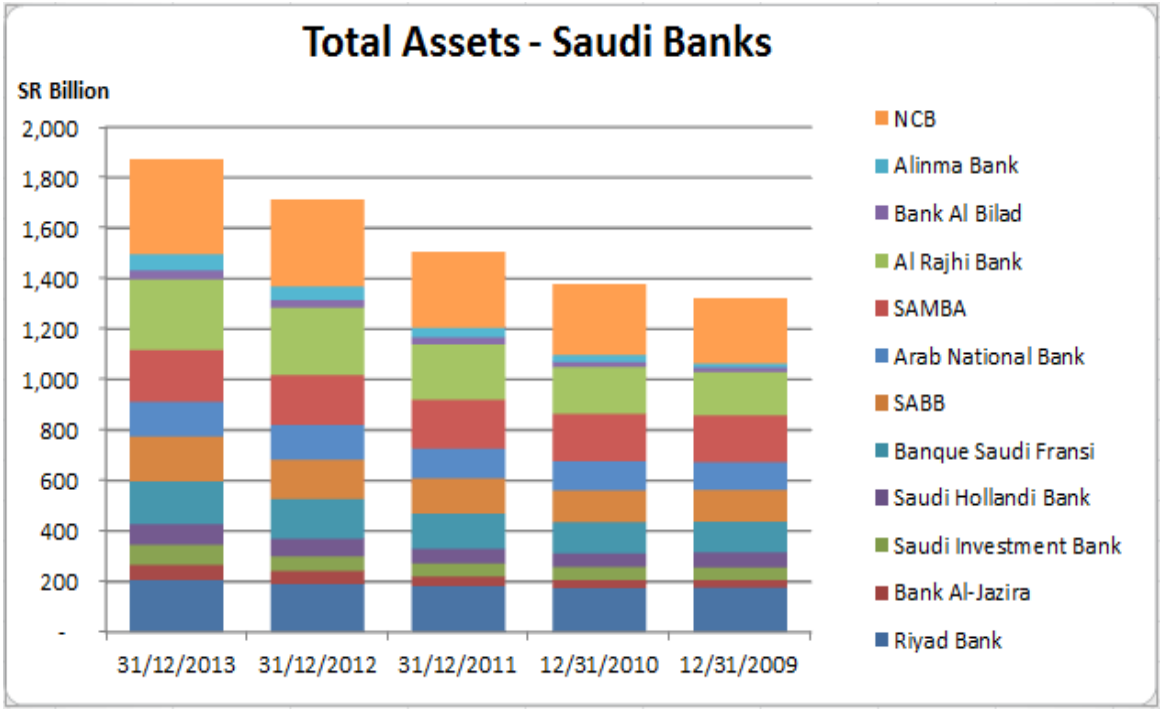


Figure 3 Total Assests in Saudi Banks (Source http://www.gulfbase.com, 2013)

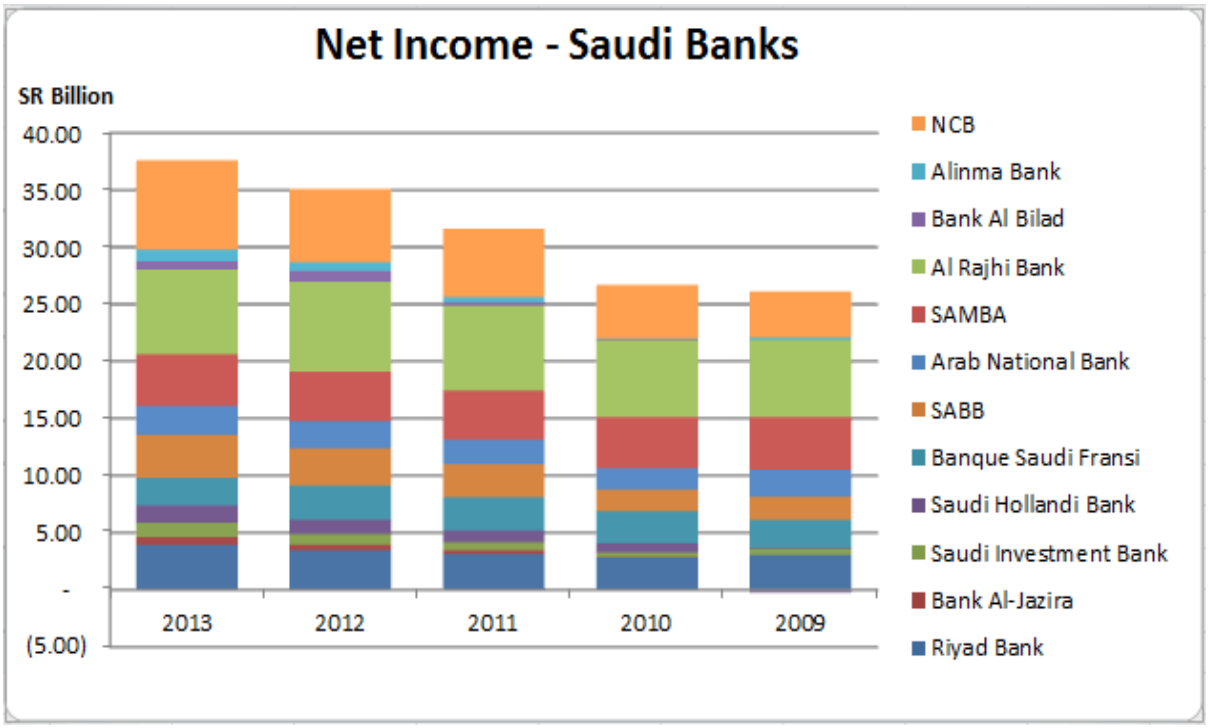


Figure 4 Net incomes in Saudi (Source http://www.gulfbase.com, 2013)

The banks in Saudi Arabia are noted for higher asset and net growth, increasing non-interest income, and a slight widening of margins, which have often resulted in higher returns for the banking sector, as highlighted in table five above. This trend has been maintained over the decade relatively with other countries in the region particularly the Qatari banking sector that has also achieved an impressive net income expansion. However, Saudi Arabia still had the highest asset growth in 2011 in the GCC (Gulf business, 2011). The banking sector in the region has also shown a steady rise in net profit from 2009 to 2013, with the region's largest banks achieving a good increase of 15.9 per cent in 2013. A large number of banks in Saudi Arabia showed this significant improvement in net profit, which strengthened their financial positions with well-maintained good capital adequacy and slightly higher liquidity.

4.8.3 Government support

The development of rules and regulations governing businesses and commerce is greatly influenced by groups such as the royal family, Islamic scholars, state officials, tribal leaders and businessmen who all have various interests and powers (Economist Intelligence Unit 2003; Al-Nodel 2004). The legal system guiding commerce and other issues of business is also based on the Islamic laws of Shariah, Alqur'an and Sunna Alsharifah, which demonstrates the high influence of Arabic heritage and Islamic values on the Saudi society (Aba-Alkhail 2001; Al-Nodel 2004). The personality and power of particular individuals and the role of family and friend relationships are noted to have much impact on regulations and the norms in the society (AlRumaihi 1997). Other major characteristic features of the Saudi business society are the domination of family businesses, influx of joint venture and foreign owned companies and the high investment and involvement of the government in business.

The Saudi Arabian government has played a key role in the provision of IT infrastructure and the establishment of e-government and e-commerce. This has earned the government the people's trust and their willingness to engage in e-commerce and Internet banking. The government has been able to enable e-retail responsibly, constructed on "three key functions: facilitation, supervision, and control '' (Algamdi *e.el*,. 2012).

People believe that the support from the government is a positive incentive and an enabler. Business people may wish to avail of this sort of business if it is

lucrative and profitable for them. However, in spite of government support, some people in the Saudi Arabia feel concern to use online facilities because of distrust towards the Internet, as the internet and e-commerce with internet banking are perceived as unknown world and processes. The government therefore sees the need to take a strong and active role in enabling e-commerce activities with full responsibilities for its control and supervision. This is designed to encourage more people and businesses to adopt e-commerce in the country. The government is also making efforts to protect customers' and sellers' rights, as government regulatory departments are being set up to obtain an overview of online transactions.

Governmental efforts are thus geared towards the provision of a motivating environment for e-commerce for both companies and individual users. To this end, the government has provided support for retailers who want to provide online sales and services. Supervision and control roles have therefore been emphasized by the government, as they are considered key success factors for online shopping in Saudi Arabia. Online shopping and e-commerce are relatively new in the Saudi Arabian environment; the government intends to protect the rights of all parties concerned. It is thus needful for clear legislation and regulations for online shopping to be established (Alfuraih,2008).

The government has also recognized that Information and Communication Technology (ICT) plays a major role in the Saudi Arabian's economy. The Saudi Arabian government has therefore, over the last decade, concentrated on supporting the provision of ICT to become the most expansive ICT platform

in the Middle East (Saudi Ministry of Commerce, 2001; Alotaibi and Alzahrani, 2003; U.S. Commercial Services, 2008). The ICT infrastructural development embarked upon by the Saudi government and the introduction of incentives and policies have been a source of big encouragement to the people and businesses of the Kingdom (Al-Tawil, Sait and Hussain, 2003).

King Abdulaziz City for Science and Technology (KACST) is officially the government arm responsible for the provision of Internet services in the kingdom. Its reported that the “Internet was introduced in Saudi Arabia in 1997, Internet users increased from one million (5% of the population) in 2001 to 11.2 million (41%) in 2010’’ (AlGamdi, 2011, p.157). This shows the expansion of Internet access in Saudi Arabia, which demonstrates its e-commerce suitability (Sait, Altawil, and Hussain, 2004). According to Ministry of Communication and Information Technology (MICT) (2010) that broadband subscriptions have also increased from 64,000 in 2005 to over 3.2 million at the end of the quarter of 2010.

A government ministry was also created in 2006 to take over responsibility for e-commerce in the country, as a way of acknowledging the importance of e-commerce and as an effort to provide the needed support from government. The Ministry of Communications and Information Technology was thus created to monitor e-commerce activities and advise government on its effective establishment. A survey conducted by the Ministry showed that the prevalence of e-commerce activities among the population in the country was 14.3% in 2008, and that on average 3.1 million Saudis have made online purchase, with

airline tickets and hotel bookings taking the major portion of these purchases (ACG 2009, AAG 2011).

4.8.4 Online Payment challange and Banking Systems in Saudi Arabia .

Online payment issues have received higher focus and attention in e-commerce activities in Saudi Arabia. The issues raised are mostly concerned with the difficulty of getting credit / debit cards, fear of card theft, which could result in financial loss, credit card fees which associated with religious issues and problems because of the interest charges from using these credit cards. These issues have presented some difficulties for most participants in e-commerce, and they have prevented many from buying online. Conditions to meet before credit cards are issued are a major concern to many, especially those without bank accounts or those not in employments (Alghamdi *et al.,* 2012).

The fear of losing one's card details or details being stolen by traders has also been a major concern for most people. The common perception is that buying online is not safe, as the use of cards exposes the user to many risks. Most people with this concern hope to see the government or the banks establish systems that will bring assurances of Internet safety.

Religious issues are also raised in the use of credit cards for online purchases. Charges and interests are taken when a credit card is used, which is known as (Riba) which defined by (Shari'a Law) as "an unjustified increment in borrowing

or lending money, paid in kind or in money above the amount of loan, as a condition imposed by the lender or voluntarily by the borrower" (debt usury), and is forbidden in Islamic law. People therefore tend to avoid online purchases using credit card (Mokhtar,*et al.,*2015)

The international acceptance of some cards and the link with internationally connected payment agencies has also been raised as issue that may prevent the growth of e-commerce in the country. The limitation of online payments methods has also remained a major issue, which the banks are addressing gradually, especially with the introduction of a system in Saudi Arabia named "Cash you". This is similar to debit cards; they allow customers to use only the money available on their accounts. However, a high fees of charge applied in order to use these type cards with each transaction therefore this can be seen as a major problem with this system, which may attract a payment of an extra fee of 100 SAR (about £16) when used to pay online (AlGhamdi and AlFaraj 2011).

4.8.5 Corporate Internet banking in Saudi Arabia

Banks in Saudi Arabia have fully embraced Internet banking, as it encourages customers to be fully involved. With the support of the government in the provision of internet infrastructures and some initial training provided by the customer relations office of the banks, most bank customers are already engaged in internet banking (Al Somali and Ghinea, 2012). Printed instructional guidelines are often given to customers, while online instructions are always on the banks' websites. The instructional guidelines focus on customers' secured

access, system integrity and security. Customers are advised to be security conscious and be protective of their data all the time. Meanwhile, the banks continually assure customers of the comprehensive guidelines put in place to ensure that their financial information is kept secured. All information is protected according to its sensitivity, and guidelines are there to serve each category of information (Samba Bank Access Guidelines, 2015) Bank staff are not privileged to access customer security detail guidelines. The banks also ensure that security checks are routinely carried out on their systems.

The bank systems are designed to provide a web-enabled online banking services facility, allowing customers to conduct several banking transactions online, in real-time and from any place. It is claimed that Internet banking provision could enable customers to focus on managing their business better with a guaranteed peace of mind.

4.9 Data Collection and Analysis

The effectiveness of research in most cases depends on how data is collected for analysis and the method of analysis. Data were collected using interviews. However, the use of any of the methods depends on the study and the advantages / effectiveness of the method. Often interviews were conducted by means of personal contact, by telephone, while surveys were issued by mail or email or posted on the website.

4.9.1 Sample Population

Saudi Arabia has twelve major financial institutions, including banks and other organisations providing financial services, operating in the country with different

branches in many cities. The Information Technology departments, Electronic commerce departments and Risk management departments of the major banks are all located in head office branches. Out of the major financial institutions, eight banks were selected to participate in the study because of their participation and heavy investment and involvement in electronic commerce and online banking.

The information technology departments, electronic commerce departments and risk management departments of the banks were also selected as participating departments, because of their direct involvement in online fraud control and their supervisory responsibilities on countermeasures. The staff of these departments were also chosen as participants in the investigation because of their knowledge of the subject matter and experience. However, due to the sensitive nature of the subject matter, getting participating organisations and their staff to take active part in the investigation proved a little difficult, but for the intervention of a contact person who is an influential senior member of staff in one of the organisations. An introductory letter presenting the aims and objectives of the research was sent to the selected banks, requesting their participation in the study. Some banks in the sample population however rejected the suggestion to participate officially, for reasons ranging from internal policies to personal issues.

4.9.2 Qualitative Data Collection and Analysis

Qualitative data were required to obtain a further, deeper, investigation, and to gain a better understanding of the subject matter. Acquiring qualitative data thus required one-to-one contact with representatives of the departments, to

obtain insider views and experiences. Thus plans were put together to interview officials of the selected departments in the participating banks. Interviews were conducted using classic Arabic language instead of ‘‘colloquial’’ language to ease the translation into English for later transcription to give an accurate interpretation.

4.9.2.1 Interview Sessions

The contact person, who was an influential senior member of staff in one of the major banks in Saudi Arabia, contributed greatly in arranging for the interview sessions by recommending the researcher to banks and selected departments. Furthermore, he helped to establish access to various department within the banks to conduct interviews in Saudi Arabia, though there was rejection from few banks due to the sensitivity of the research refusing to disclose information with regards to online fraud .The final interview plan and schedule, showing staff participants, bank, data and times of interviews, included thirty-five staff in six Banks.

However, twenty-seven interviews were carried out with staff in four banks, who agreed to participate in the investigation. The participants were selected according to their functions in the banks and roles in the prevention of online fraud in their respective banks. The analysis process involved coding. The coding process is a recursive process that involves phases, including familiarisation with the data / transcription of the verbal data, generation of initial codes, searching for themes, reviewing the themes, defining and naming themes and report writing (Braun and Clarke, 2006). The transcribed dataset was read through carefully for better understanding, and notable highlights / sentences relating to the study objectives were given unique codes. The

relationships between the codes identified were then used to group the codes into sub-themes and themes, which were used for the presentation of the data analysis and discussion. The identified themes were perception, awareness and technological measures; regulations; and enforcement.

Participants	Position / Function	Number interviewed
IT Bank staff	Risk managers	10
	IT technicians	3
Customer services	Services Managers	4
	Account Officers	4
Bank Customers	Account owners	3
Government regulators	E-commerce supervision	3

Table 4 Participants for interview

4.9.2.2 Qualitative Data Analysis

Qualitative data may be analysed using a variety of approaches embracing the rigour of science, procedures and the creative elements of emergent discovery, highlighting the interpretive nature of qualitative data analysis (Hennink *et al*., 2011). The approaches open to use for this study include content analysis, thematic analysis and discourse analysis, which can all provide scientific and artful qualitative analysis to enhance useful interpretation of the datasets collected (Patton 1990; Corbin and Strauss, 2008). The approaches used established methodological procedures and well-accepted techniques, useful in different situations and purposes (Hennink *et al*., 2011; Attride-Stiling, 2001).

The thematic analytical method is the chosen method for qualitative analysis for this research, which collected textual data through semi-structured interviews. It is flexible, allowing the researcher different options and techniques to pick or untangle the reality in any situation (Braun and Clarke, 2006).

4.9.2.3 Thematic Analysis

Thematic analysis is readily applicable in various situations and used in different forms (Boyatzis, 1998; Braun and Clarke, 2006). It can be seen as a method but sometimes as process because of the activities involved which may be iterative (Ryan and Bernard, 2000; Braun and Clarke, 2006).

The thematic coding element is essentially useful in organising the datasets collected during interviews as it helps in presenting the richness of the data in different pattern and themes. Its adaptable uncomplicated method for qualitative research gives a theoretical and flexible approach to qualitative data analysis, which is independent from theories, in contrast with other analytical methods that are theoretically based, such as interpretive phenomenological analysis (IPA), discourse analysis and grounded theory, (Stauss & Corbin 1998; Willig, 2003; Smith & Osborn, 2003). The form of the thematic analysis depends on the approach in terms of what constitutes a theme and how to present the richness of the dataset. This is usually done using an inductive or bottom-up approach, or a deductive theoretical or top-down way to identify themes. The flexibility of thematic analysis and the absence of rigid rules give the researcher power to determine what a theme is. Judgement is usually based on whether the theme captures an important aspect in relation to the overall research question. The flexibility also enables the researcher to decide

if the analysis would reflect the entire dataset or a particular aspect. Focusing on the entire dataset allows for a rich thematic description, but may lack some depth, while focusing on one aspect of the dataset provides opportunity for in-depth analysis.

Other areas of flexibility that determine the form of analysis include the ability of the researcher to choose the ways themes within the data can be identified. This decision is based on linking the themes to the theoretical framework (theoretical / deductive or top down) or just the data (inductive or bottom up) (Patton, 1990; Boyatzis, 1998; Hayes, 1997). Inductive analysis is therefore data-driven, where the researcher codes the data without a pre-existing coding frame, usually based on a theoretical framework. It provides a rich description of the overall data, whereas deductive analysis is theory or analyst driven, and the process of coding the data is made to fit into the theoretical framework of the research. In this process, the focus of the researcher may be on particular aspects of the data that relate to the theoretical framework. There could therefore be a possibility of missing out on the full richness of the entire dataset. The process of coding is therefore an important aspect of thematic analysis.

4.9.2.4 Transcription of Data and Coding

The data set gathered from the 27 participants' recorded interviews of one-hour duration each were transcribed while focusing on retaining sufficient details of the interview, which enhanced the recording of the near verbatim account of the interviews. The transcription process therefore involved a replay of the recorded interview, coupled with a confirmation of the interview notes and

matching any observed actions or happenings during the interview session. The rationale is to recreate the interview sessions, to gain a better comprehensive knowledge of the dataset. This produced a deeper understanding of the data and the issues involved which helped to formulate the initial development of ideas and patterns in relation to the data (Riessman 1993; Lapadat and Lindsay, 1999). The transcripts for the individual interview sessions were later compared individually against the interview recordings to ascertain the validity and accuracy or omission of any data.

The coding process was highly influenced by the understanding gained of the dataset during the transcription stage. Initial codes based on the objectives of the study were given to issues and patterns identified in the dataset. Codes were also deduced from the dataset as new issues or patterns outside the stated objectives were highlighted. This was done to ensure that the datasets were comprehensively covered and that the every issue or pattern related to the study objectives or not are identified and appropriately covered.

Using Microsoft Word, transcript texts relating to some issues and objectives were highlighted and tagged with unique codes to indicate a pattern (Braun. and Clarke, 2006). At the end of the coding and the dataset, text with similar codes were segregated and grouped together to form initial themes representing the different aspects of the study findings that would enhance better explanation (Grbich, 2007).

The emerging groups of codes forming the themes were thereafter checked individually for duplication, relevance and relationships with other groups. This checks and crosschecking across the groups/themes resulted in the regrouping into sub themes and final themes. Consequently five major themes were identified with twelve sub-themes, as indicated in chapter 6 Table 13.

4.10 Conclusion

This chapter has reviewed the motivation and nature of the research in the context of the objectives and the socio-cultural context of the subject matter to determine and justify the suitable research approach chosen. The chapter also highlighted the research design using case study and a mixed data collection technique to collect qualitative data. The next chapter reviews the datasets and presents the analysis of the data sets qualitatively.

CHAPTER 5

QUALITATIVE ANALYSIS AND FINDINGS

This chapter presents the analysis of the qualitative data set collected during the empirical investigation through semi- structured interview sessions (see details in section 4.9.2 and the findings. Five major themes were identified with twelve sub-themes, as illustrated in Table 10 below.

The themes and the sub-themes enhanced the effective organisation of the dataset and in in presenting the richness of the data. A deductive theoretical or top-down approach was used to identify themes which are linked to the theoretical framework highlighted in chapter 3. At the same time, because of the flexibility of thematic analysis and the absence of rigid rules which allows for easy determination of a theme, an inductive or bottom up approach which is purely data driven was also used to provide a rich description of the overall data. The inductive or bottom up approach allowed the coding of the data without a pre-existing coding frame, but was guided by the objectives of the research and the theoretical framework.

The coding of the data was rigorously carried out using a standard scientific approach strongly enhanced by the knowledge of the dataset and the objectives of the research. Moreover, using the deductive approach, codes were given to patterns or common issues / occurrences in the datasets which were identified or seen to be related to any of the objectives of the research. To ensure the identification of all issues or patterns in the dataset irrespective of their relationship with the set objectives of the research, an inductive bottom up

approach was also used to examine the dataset more comprehensively. This was aimed at picking or untangling the reality in the situation under investigation (Braun and Clarke, 2006). This process allowed a manual cross-checking of the datasets, the issues / patterns identified and the objectives of the research. It also allowed a better understanding of the dataset and provided a platform to appreciate, fully utilise and present the richness of the dataset in a formal way for easy analysis and interpretation. It provided a platform for scientific and artful qualitative analysis aimed at enhancing useful interpretation of the datasets collected (Patton 1990; Corbin and Strauss, 2008). It also shows the flexibility and ability of thematic analysis to embrace the rigour of science, procedures and the creative elements of emergent discovery of useful and meaningful knowledge which highlights the interpretive nature of qualitative data analysis (Hennink *et al*., 2011).

The coded datasets or identified patterns were later segregated and grouped together on the bases of their relationships, to form initial themes representing the different aspects of the research framework and objectives. These groups of coded dataset that formed the themes were thereafter iteratively checked individually for duplication, relevance and relationships with other groups. The checks and crosschecking across the groups/themes later resulted in the regrouping into sub themes and final themes. Consequently five major themes were identified with twelve sub-themes, as indicated in Table 10.

Themes	Sub-Themes	Codes
Perception	Definition of online fraud	Technology based/inspired/driven Game deception
	Perception of online fraud	Criminal activity Anti-social Greed/hunger/not criminal
Awareness	Level of awareness	Lack of knowledge Training Lack of government sensitisation Religious inclinations
	Frequency of occurrence	Personal experiences E-commerce activities Reporting status
Technological measures	Technological controls	Computer controls Procedural controls and checks Complex/Cumbersome operations Ignorance/vigilance
	Control focus	Abuse/unlawful use of computing resources Protecting confidential information of customers Illegal online activities

	Relevance and adequacy of measures	Safe and trust worthy Involvement of the customers Regular updates needed
Regulations	Types of regulations	Government regulations/laws In-house rules and guidelines
	Focus of the regulations	Internet monitoring Operational guidelines
	Impact of the regulations	Lack of awareness Lack of focus and purpose Need for internal rules
Enforcement	Prosecution of offenders	Passive enforcement Socio-cultural and infrastructural handicaps Lack of knowledge/experience
	Preparedness of agencies	Training Infrastructural base

Table 5 Theme, sub-theme, codes of qualitative data

5.1 Perception

This theme identified the meaning of online fraud and how the people see or perceive online fraud based on their cultural and societal beliefs and educational background Table 13. Two sub themes will be discussed in this section. The sub theme online fraud definition has three codes that capture the meaning of online fraud as given by the participants. The codes are technology based/inspired/driven definition; game based definition; and deception based definition. The second sub theme looks at the perception of the people and how

they regard online fraud. It has three codes capturing the way the participants see online fraud as a criminal activity, anti-social, and greedy and hunger driven activity and not a criminal activity.

Theme	Sub-Themes	Codes
Perception	**Definition of online fraud**	Technology based/inspired/driven Game Deception
	Perception of online fraud	Criminal activity Anti-Social Greed/hunger/not criminal

Table 6 Perception Theme

5.1.1 Definition / Meaning of Online Fraud (Sub-theme)

The interpretation of the participants as regards the meaning and definition of online fraud shows three main definitions and classifications. Participants generally agree that online fraud is technologically driven and inspired, it is a game played by two or more players to outwit one another, and it is a life of deception based on lies and tricks using technological skills.

5.1.1.1 Technologically Driven and Inspired

Online fraud is essentially a computer mediated/ computer engineered activity, which can only be carried out using computers, participants believe that e-commerce technologies is changing the way we communicate, with less human involvement as well as less interactions .

"People do all sorts of things with the emergence of technology which can hide their nefarious activities. The technology particularly the mobile technologies/devices makes them faceless and a cover to deceive their unsuspecting victims" (B2)

"Online fraud simply means fraud engineered, executed and perfected with the use of the computer and its devices….it involves the use of stolen credit/debit cards, giving false information during online transactions, identity theft or unauthorised access to computing resources" (B1)

The increase of online fraud is therefore attributed to the increased application of computers and its devices which has become the foundation and the driving force of online fraud in the country

"Because most businesses are now done online, fraudsters are now using their computer skills and resources for their selfish interests and gains" (B26)

Online fraud is therefore described as computer-aided fraud.

"Online fraud is simply fraudulent practices perpetrated online with the use of computers…it can be described as a computer aided fraud or a technology backed fraud and therefore can only involve computer literates who use or rely on the computer for their daily businesses" (B5)

Because online fraud is believed to be computer aided, the opinion of the participants is that only computer literates and technically skilled people perpetrate such fraud, and mostly for selfish interest and destructive purposes.

"I see online fraud as a fraud committed with the aid of a computer, so it is for the educated and westernised people who have imbibed the culture of the west. The common man cannot be involved in such a crime" (B3)

"Online fraud is destructive with a mission to hurt an organisation by gaining access to vital data on computers for selfish desires and making the data unusable for the organisation" (B6)

Participants agree that lack of knowledge of computer and related technologies could be a major reason people fall victim to online fraud. Most people with computer knowledge and ability to use computer on their own can detect fraudulent practices. Therefore computer training should be given in schools and other places.

> "*Fighting online fraud which is computer assisted requires extensive computer knowledge and up-to-date training. This training is required in this modern age to fight not just online fraud but all other crimes in the society. Organisations, clubs and other societies should be able to encourage their members to be computer literates*" (C2)

Therefore the level of awareness towards the issue of online fraud seems to be inadequate and not given any seriousness. The government and the financial

institutions have not done much to sensitize their customers and the general public.

> "*Online fraud is embedded in the technologies used in banking and other financial transactions and therefore may be hidden from a lot of innocent people especially our customers, it is thus our duty to inform them of its dangers and educate them on ways of avoiding being victims" (B1*)

The seriousness of the dangers of online fraud also relates to the innovations of the technologies used. Participants agree that the rapid changes in the technologies used makes obsolete the systems that staffs are used to, most staffs may not also have knowledge of the new systems.

> "*The banks need to be proactive and be current with technological changes in the industry. Staffs also need to update their knowledge through training and workshops*" (B4)

5.1.1.2 Online Fraud as a Game

Most participants also describe online fraud as a game played by computer whiz kids to show their ingenuity aimed at outwitting their competitors.

> *"It takes the ingenuity of a computer and sometimes the foolishness and careless of the victims to see the occurrence of online fraud" (B8)*

Participants therefore agree that the schools, government, religious leaders and other societies have roles to play in making people computer literates, be contented in what they have and live harmoniously with their neighbours.

"Because the computer is involved in this online fraud it will be wise for everyone to have computer training to be smart, at the same time since greed is also involved, society should discourage this behaviour" (C3)

Some participants also agree that online fraud is a way of showing cleverness of some people who derive joy in proving themselves better and smarter than their competitors in terms defrauding others.

"Fraud is a natural issue in business where one partner tries to be smarter than other partners when false information is used" (B21)

"I therefore see online fraud as a game played by the big men in the society using their technological resources to outplay one another; it is a game of the winner takes it all, and the smarter ones always win" (B9)

This suggests that the motive of online fraud could be to show cleverness and self-satisfaction on the part of the criminals for outsmarting others and achieving technological advantage.

5.1.1.3 Online Fraud as Deception

Fraudsters take advantages of online users' trust, deceiving them through their knowledge and skills for instance, they can attract users through ''sales tricks" such as very low price goods and reduced offers.

"Online fraud is a devilish calculated and carefully planned act to steal by fraudulent means using advanced technologies" (B7)

"Any activity to deceptively gain possession is regarded as anti-social and against our cultural values" (B27)

5.1.2 Perception of the Participants on Online Fraud

Participants see the implications of online fraud activities from different perspectives. Home computer users browse the Internet with a false sense of security, depending on the built-in firewalls and antivirus tools that may protect them from a cyber-attack. Online industries still use email messaging to reply to customers; once their customer's email has been hacked, the organisations could be communicating with the hacker instead of the client. It is in the best interest of the global community to start training users on their cyber vulnerabilities, including how their clients can start protecting themselves.

5.1.2.1 Criminal Activity

The perception of most participants is that online fraud is a criminal activity. The two issues mainly highlighted in the categorisation of online fraud as a criminal activity are the intention or mission of the act and the means or method used.

"Online fraud depends on the mission of the actor and the means used to carry out the mission, sometimes it could just be an attack on our computing

resources, a personal vendetta or a calculated effort to steal using the devices of the computing systems" (B23)

The general mission and intention of a crime is to create havoc, attack and destroy facilities and to steal or unlawfully gain possession of something of interest to the perpetrator.

"Online fraud is surely a criminal activity because the fraudster has a criminal intention to commit havoc on another person or an organisation" (B4)

"Online fraud to us is a direct attack on our computer resources and an indirect attack on the wealth of our customers" (B18)

"Online fraud is a wicked act and the perpetrator must be treated as an armed robber" (B6)

"A hungry man who steals to eat cannot be condemned or tagged a thief, those who go about stealing by deception are hungry people and as long as it is not against the county and government I will not label them criminals" (B9)

The consensus of the participants regarding the means used to perpetrate the online fraudulent act is that the means or method used is inconsequential.

"A fraud is a fraud whether committed using pen, gun or computer, and a fraud is a crime … I therefore see online fraud as a crime which should be punishable by law" (B1)

"A person caught robbing a bank with a gun is branded a criminal, I think it should be the same for anyone stealing from the bank with a computer device" (B7)

The other major issue highlighted in the findings is the position of the law and the government and the classification of online fraud. Most participants are of the opinion that the law of the land should be very clear on classifying online fraud as a crime and that the law should take its full course on any such act.

"It is a criminal activity and should be punishable by law, but this depends on how the law of the land may see it, in other countries where there are special laws for technology driven crimes, online fraud is clearly designated a crime" (B2)

"The law of the land describes stealing as a crime therefore online fraud which involves stealing is a criminal activity" (B24)

"Online fraud is simply a fraud at a high and sophisticated level; I see it as a crime even if the government regulation is not specific about it" (B25)

Most participants acknowledged that the laws may not be very clear on some criminal activities and therefore requires the government to make laws specifically to stipulate the nature of the crime and punishments. It was also agreed that most of the laws are not well known nor understood by the general public and therefore more sensitisation of the people through publicity, teachings and training by government, public institutions, schools and religious organisations need to be done.

> *"Most of the public are not aware of online fraud as a crime, as no clear definition has been given by the government or any other responsible organisation. There should be ways of creating awareness in the schools, and other public places" (C2)*

5.1.2.2 Anti-Social

Most participants also agreed that online fraud is both socially and culturally out of order and does not represent the socio-cultural and religious beliefs of the nation. This is because the main reason of communication for a fraudster is victimise online users.

> *"Any activity to deceptively gain possession is regarded as anti-social and against our cultural values…online fraud is one of such activities" (B21)*

"Our religion also preaches that stealing or deceiving your brother is wrong and anti-Islam and is punishable irrespective of the means or methods used" (B5)

The perception is that because the culture and social norms of Saudi Arabia condemn stealing of any kind, online fraud is seen as a social taboo and a social crime.

"People here see online fraud as a taboo and a religious defilement, even the victims are reluctant to report it for fear of being implicated" (B8)

"We are cultural minded people and we tend to see things in the light of our culture and religion…stealing and defrauding one another is a social crime in our culture we therefore condemn anything of such including online fraud" (B2)

Some participants also suggested that because people are culturally mined and do things in the light of their religion, this culture and religious sensitivity should be used to direct and mould the peoples' mind-set against any kind of fraud. The religious leaders may have a big role to play in providing necessary teachings and counselling.

> *"Our religious sensitivity need to be exploited as most of us dogmatically follow the teachings of our spiritual leaders, teachings should be more focused on the vices of fraud and other criminal activities" (C3)*

5.1.2.3 Hunger-induced Non-Criminal Activity

The findings also suggest that the intention or the motive of the activity may determine how it is classified. Some participants therefore do not see fraudulent practices based on hunger as criminal, but rather as a social problem that needs to be addressed socially.

"If a man is hungry and steals food, he cannot be tagged a thief, we are obliged to help the needy and correct the anomalies and imbalance in the society" (B6)

"A hungry man who steals to eat cannot be condemned or tagged a thief, those who go about stealing by deception are hungry people and as long as it is not against the county and government I will not label them criminals" (B8)

Other participants also attributed the occurrence of online fraud to the greedy get-rich-quick attitude of the victims. It is agreed that it 'takes two to tango', and that the welcoming posture of the greedy victims make room for the perpetration of online fraud. They therefore cannot claim a crime has been committed against them.

"I also blame the victims who most times because of greed open up themselves for such deceitful acts, but as long as the online fraud activity is not

against the county, innocent law abiding citizens, and government I cannot see it as a crime" (B15)

5.1.3 Theme Summary

The findings therefore show that online fraud is described as a deceptive act carried out by IT-skilled people using their knowledge and the power of the computer to satisfy their selfish desires. It is therefore seen as a normal business affair carried out at a technological level, which limits the type of players to smart computer literates, and differentiates the winners from the losers by their level of knowledge, skills and carelessness. These backgrounds formed the different opinions and perceptions of online fraud of the people. The findings therefore suggest that, based on these cultural and social backgrounds, online fraud is a criminal activity and a social crime, but if it is inspired or driven by hunger or the greedy aspirations of the people, then online fraud cannot be seen as a criminal activity.

5.2 Awareness Theme

This theme acknowledges the importance of awareness, the issues surrounding the levels of awareness and the challenges these issues pose to online occurrences of fraud in the country Table 14. The data set highlights seven codes which capture the issues and challenges confronting awareness and online fraud. These codes are grouped into two sub-themes, which are discussed in this section. The sub-themes are the level of awareness with four codes namely lack of knowledge; training; lack of government sensitisation;

and religious inclinations, and frequency of occurrence with three codes namely personal experiences; E-commerce activities; and reporting status.

Theme	Sub-Themes	Codes
Awareness	**Level of awareness**	Lack of knowledge
		Training
		Lack of government sensitisation
		Religious inclinations
	Frequency of occurrence	Personal experiences
		E-commerce activities
		Reporting status

Table 7 Awareness Theme

5.2.1 Level of Awareness

The findings showed that the level of awareness of online fraud is low in Saudi Arabia. This could be attributable to four issues identified, namely lack of knowledge; training; lack of government sensitisation; and religious inclinations.

5.2.1.1 Lack of knowledge

Most participants agree that the low level or complete lack of knowledge of online fraud and online fraud activities may be due to their level of education and exposure to computers. The findings also show that the fraudsters took advantage of the victims' ignorance and their dependence on guidance.

"I would say most of us have fallen victims of what we do not know, we have fallen prey to online fraud due to our lack of knowledge or awareness of online fraud practices" (B1)

"Due to our culture and religious orientation, most of us are ignorant of online fraud and the activities of fraudsters. Our educational level may also have contributed to this low level of awareness; most of us cannot read nor write not to talk about using the computer" (B6)

Participants highlighted the issue of their low educational level that has contributed to their ignorance, lack of awareness and perception on online fraud. Those participants that are moderately educated also highlighted the need for knowledge update and training on modern technologies.

> "The increasing rate of online fraud need to be stopped by massive investment in education and training, schools and organisations should be actively involved in this" (B2)

The findings showed instances where ignorant computer illiterates unsuspectingly gave out their bank cards and details to relatives or friends to help carry out some financial transactions, and were defrauded with the use of such account details by these relatives or friends purporting to be the original account holders.

"I wonder how they expect us to be discreet about our account details when we have to call on family members and friends to use our cards for us in many transactions, the banks should consider our plights and device means and procedures to help our situation" (B8)

"The tactic is basically to lure the victims into giving their account details or other confidential details which will now be used to gain access to the victim's accounts or assume the victim's identity in illegal transactions" (B24)

"We have experienced various attempts by dubious people in the last two years to use fake identity to gain access to funds in some accounts, we have also received complaints from customers who paid some money into business accounts in our banks, with the hope of receiving goods promised, but did not receive any" (B3)

Participants also agree that their perception of online fraud influences their knowledge and consequently their awareness. Most of the participants have only heard of computer hacking and physical attack on computing facilities, and, as such, have limited knowledge of online fraud. Thus most participants highlight the need for government and society to ensure that the people are well educated on technological advancements and challenges it brings.

"What is not tagged a crime cannot be seen as a crime and therefore cannot be combated, I am only aware that computer hacking or phishing attack on computer databases/software are computer crimes, but maybe I am better educated I would have known better" (B18)

However, the findings also indicated that, as people became more knowledgeable and more exposed to international business, their level of

awareness of online fraud increased and they were more cautious. It reveals that those who are knowledgeable are less likely to fall prey to the fraudsters.

"Due to my educational background and exposure or involvement in international business, I am very much aware of online fraud, the tricks and the gadgets used" (B9)

"The awareness level is increasing; the citizens, business organisations and the government are beginning to be more knowledgeable on the activities of online fraudsters" (B22)

"People are increasingly aware of online fraud which is a positive sign for effective fight against online fraud. The more people know about online fraud the less it is to fall victim to online fraud" (B5)

Most participants therefore agree that one effective way of combatting the increase of online fraud is education and regular updating of knowledge.

5.2.1.2 Training

The findings showed that some participants think that training and education have been used to create the necessary awareness of online fraud. The effect of this has also been positive on the fight against online fraud in Saudi Arabia. Some organisations and even private individuals have used training to expose the tricks and games of online fraudsters. However, there is a conflict of opinions surrounding this issue.

"The in-house training has made me aware of the tricks of online fraudsters, the technologies installed in our organisation and the procedures

any transaction should go through have also increased my knowledge of online fraud activities" (B7)

"My knowledge of the tricks has helped me avoid fraudsters and has never fallen as a victim .I also try as I can to educate my friends who use computers on how to identify and avoid fallen into their traps" (B19)

Training and education are carried out in-house for both staff and customers, using company social media, and customer service advice is usually given over the counter during account-opening transactions or e-commerce transactions.

"We have used our in-house training and marketing campaign on online banking to create necessary awareness aimed at keeping our staff and customers from becoming victims or collaborators, however more technical training for staff and IT / customer risks training need be given and intensified" (B4)

5.2.1.3 Lack of Government Sensitisation

The study shows that the lack of government sensitisation contributed to the low level of awareness and the consequent rise of online fraud in the country. The government's relative silence on the activities of online fraudsters more or less created an impression that online fraud is not a crime.

"I am not aware of any regulation from the government nor of any government activity warning online users of online fraudulent tricks, therefore

do I find it difficult to know when a crime is committed. It is also apparent that the government has not qualified online fraud as a crime" (B1)

"What is not tagged a crime cannot be seen as a crime and therefore cannot be combated, the people need to be clear on the government stand on this issue and as such requires to government to provide training for the citizens" (B13)

However, as the cases of online fraud increased in the country, the government focus shifted from just monitoring internet usage to a publicity campaign about online fraud.

"The awareness level is increasing; the citizens, business organisations and the government are beginning to be more knowledgeable on the activities of online fraudsters. The government on its own is sensitising the people and government agencies to be battle ready for the menace of online fraud in the society" (B16)

"I expect the government to mount a serious campaign through publicity and training against online fraud involving all the stakeholders in the financial industry"

5.2.1.4 Religious Inclinations

Most participants agreed that their cultural and religious background might have affected their level and sense of awareness in relation to online fraud in the country. There is a consciousness to do good to people around you all the

time, whereby evil vices and practices are not expected from anyone at any time.

"Due to our culture and religious orientation, most of us are ignorant of online fraud and the activities of fraudsters" (B27)

"The country is a peaceful and very religious nation where fraud and theft is a taboo, we don't hear of such vices often, so online fraud is not common and you are daily reminded of the evil such vices bring to the family" (B9)

Participants thus agree that religious and cultural leaders need to be involved in the fight against online fraud through religious teachings and evolving cultural and social norms.

"Because of my religious background, I will always follow the teachings of my religious leader" (C2)

Another reason why there is a low level of awareness is the fear held by the victims of being attacked by the community for committing a taboo that is anti-social. Victims quietly live with this frightful experience of being defrauded and not getting help because of the prevailing religious beliefs.

"Because people here see online fraud as a taboo and a religious defilement, even the victims are reluctant to report it for fear of being implicated. This makes it difficult to know the actual number of the crime and also to raise necessary awareness; I will expect the social clubs and other

religious organisations to counsel their members and enlighten them on the dangers of online fraud and encourage them to fight it" (B7)

To increase the level of awareness of online fraud, greater attention by the religious authorities and social clubs are required for a social and religious orientation so that it is no longer seen as a taboo among the people.

5.2.2 Frequency of occurrence

This sub-theme captures the issues regarding the occurrence of online fraud and the challenges faced by the institutions and the victims. The findings identified three main issues affecting the frequency of occurrence and, subsequently, online fraud in the country. The issues are the personal experiences of the people involved, E-commerce activities, and reporting status.

5.2.2.1 Personal Experiences

The findings showed that most people with personal experiences are those in business and those involved in e-transactions. It showed that the business community is becoming more aware of online fraud as they engage in e-commerce activities, and fall victims to the fraudulent practices of online fraudsters.

"I have personally not experienced any online fraud but I have seen my business partner duped twice during online purchases" (B26)

"As a businessman I see a lot of fraudulent transactions and attempts by fraudsters to dupe the ignorant ones and those that are greedy and careless .this trend is increasing especially with more people and business organisations engaged in e-commerce and the use of computers for many business transactions" (B21)

The majority of online fraud cases reported are also business cases, signifying the prevalence of business-related fraud as the major type of online fraud. Most fraud is reported to have targeted unauthorised access to the business accounts of persons using a false identity. Most participants agree that this may have caused an increased awareness of these types of online fraud.

"In the last three months I have received bogus emails suspected to have criminal intentions of seeking access to my confidential details; I have also had one or two occasions where an email reported payments into my bank accounts from unknown persons which happened to be false but attempts to access my bank accounts" (B4)

"It is becoming a daily occurrence as our customers are increasingly engaged in online transactions, some have paid money to fraudsters who have deceitfully collected money but sent no goods" (B8)

5.2.2.2 E-Commerce Activities

Participants agreed that there is an increase in electronic transactions, as the government encourages the adoption of ICT in different aspects of governance and the economy. The involvement of more people in electronic business has thus opened up the challenges and problems usually associated with ICT

adoption. This has therefore increased the awareness of online fraud and other dangers of using e-commerce.

"I encounter online fraudulent advances almost every month, it initially was about once in every year, but since the government introduced e-governance and encouraged e-commerce, the prevalence of online fraud has increased" (B1)

Participants also agreed that the introduction of electronic banking to facilitate the easy use of banking services for the customers also opened avenues for fraudulent practices. Fraudsters prey on their victims' ignorance and carelessness ,e.g. by stealing their bankcards and other confidential details.

"Online fraud is fast becoming an everyday occurrence as more people use our online banking systems and are equally encouraged to report any fraudulent activity" (B5)

"We have encountered in our bank online fraud an average of three per month, most of the cases reported are identity theft cases, resulting from the carelessness and ignorance of our customers … to this effect an awareness campaign has been launched to keep our customers well informed" (B14)

5.2.2.3 Reporting Status

One major issue that may have affected the level of awareness of online fraud is the amount of reporting to the regulating authorities of online fraud cases by the victims. The findings showed that victims are reluctant to report incidences

of fraud against them for many reasons. The failure or refusal to report online fraud has kept many likely victims in the dark and does not create the necessary awareness. Social clubs and other organisations could help in informing their members of the benefits of reporting cases such as helping to stop the criminal and creating the awareness needed to avoid others falling prey.

"Because people here see online fraud as a taboo and a religious defilement, even the victims are reluctant to report it for fear of being implicated. This makes it difficult to know the actual number of the crime and also to raise necessary awareness. Social clubs that help shape societal norms may help with counselling and support to victims" (B3)

"Our major concern is the refusal of victims to report online fraud and the fraudsters involved…we are still getting few reported cases monthly" (B7)

""People also fear to report online fraud in case they become involved in an investigation that may intrude on their privacy. The banks and law enforcement agencies need to reassure the victims of their privacy and necessary support '' (B12)

The failure of victims to report cases is also attributed to be due to a lack of proper confidential reporting procedures / systems. Major Banks have therefore been attempting to introduce reporting structures to encourage victims to use available platforms to report and fight online fraud.

"Online fraud is now being reported on the average of five per month. But we believe that a lot more is happening, the people are not just ready to report incidences maybe due to lack of trust on the government to help them out or the fear of their involvement, we are encouraging victims to help combat the crime by coming boldly to report issues like online fraud. There is need to set up a reporting structure that victims will have confidence in to report any case" (B19)

"These regular occurrences are disturbing and have made us in the bank to introduce measures to prevent them, first by getting the right picture of the situation as victims use our measures and procedures to report fraud and give details of the fraudsters" (B12)

5.2.3 Theme Summary

The findings showed that awareness of online fraud is a major issue that may affect its prevention in the country. The level of awareness was low, due to a lack of knowledge, training, lack of government sensitisation and the religious inclinations of the people. Meanwhile the frequency of occurrence is increasing, owing to the increased activities of e-commerce, although accurate figures may not be known, because of the reporting structure that has seen many victims fail to report online crimes.

5.3 Technological Measures Theme

This theme covers the investigation of the technological measures in place to check and control online fraud in the country (Table 15). It reflects issues that

relate to the types of technological and procedural controls, how these controls are designed, their main targets or focus and the relevance or adequacy of the controls. Three sub-themes are identified, namely technological controls; control focus; and relevance / adequacy. Three sub-themes are identified namely technological controls; control focus; and relevance/adequacy.

Theme	Sub-Themes	Codes
Technological measures	**Technological controls**	Computer controls
		Procedural controls and checks
		Complex/Cumbersome operations
		Ignorance/Vigilance
	Control Focus	Abuse/Unlawful use of computing resources
		Protecting confidential information of customers
		Illegal online activities
	Relevance and adequacy of measures	Safe and trust worthy
		Involvement of the customers
		Regular updates needed

Table 8 Technological Measures Theme

5.3.1 Technological Controls

The findings showed that most banks and other organisations, including the government, have realised the enormity of online fraud, and have taken steps to stop the increasing trend. While some organisations relied only on

technological controls, others emphasised the use of procedural and process controls and others a mixture of technology and procedural controls. Nevertheless, the installation of these measures somehow makes most operations more complex and cumbersome, and may require the vigilance and understanding of the operators and customers.

5.3.1.1 Technology and Computer Controls

One basic measure taken is the installation of technological systems relied upon by most organisations because of the technological driven nature of online fraud.

"Because online fraud is technology based and enhanced by current technologies, the best way to fight it will also be through cutting edge technologies, we have taken steps in the right direction to acquire these technologies to fight online fraud and other associated crimes in the bank" (B15)

Participants also agree that there are different technologies designed to prevent and detect online fraud and other related computer crimes and fraudulent practices, which are now put in place in some organisations.

"We have some technological infrastructures to help monitor and detect illegal use of the internet for fraudulent practices" (B23)

"There is a monitoring system put in place by government to monitor online activities" (B5)

Most participants also believe that organisations have the obligation to protect their customers' assets and trust and are therefore responsible for installing appropriate measures to meet these demands.

"Every organisation have a way of securing their assets and database, we have technological gadgets, software programs and procedural controls" (B4)

"We are a global bank with heavy transactions in billions of dollars and therefore cannot afford to lose our database to any hacker or fraudulent practices. We have therefore put in place state of the art infrastructures to protect our data and our customers" (B3)

Others, however, put the responsibility of protecting both citizens and organisations in the country on the shoulders of the government and the institutions directly connected to e-commerce.

"It is the responsibility of the government and its agencies to protect its citizenry against theft and other criminal activities. Laws needs to be made against such and necessary penalties defined to deter anyone, it is not our job to fight crime, but we can only protect ourselves" (B8)

"Yes we have technological systems to mainly check against unauthorised access to our computing resources but unfortunately our focus

has not been on online fraud which is usually associated with e-commerce. We believe the organisations involved in that should come up with systems to protect their customers from such online fraud" (B27)

However, participants also agree that although organisations have taken bold steps in adopting technological measures, the training for staff and awareness on the part of the customers need to accompany the installation of the measures for effectiveness.

> *"The adoption of the technological measures are good but what is equally important to make it work and achieve its purpose is the training required for the staff and the social procedures that have to be in place to inform and reassure the customers and public" (B19)*

> *"Both the organisations introducing the technological measures and the governments should educate their staff and the general public to create a viable environment for online transactions" (B7)*

Participants also agree that most financial organisations have adopted the technological measures as a result of the industry practices which seem to set standards. These practices or standards have a way of influencing the types of measures adopted by the organisations.

> *"We observe the influence of the industry in the ways organisations are adopting and putting in place countermeasures, this implies that the industry body with oversight for banks should be able to direct the fight against online fraud" (B12)*

5.3.1.2 Procedural Controls and Checks

The findings also showed that most organisations rely strongly on procedural controls and checks to prevent and detect online fraud. These organisations suggested that most online fraud is a result of loopholes in the procedures, which fraudsters take advantage of regularly, and also due to lack of proper checks.

"Most organisations have put in some control measures to confirm transactions before instructions are carried out. These have helped in many ways to detect and prevent fraudulent activities but have not helped much in deterring fraud" (B7)

"A lot however depends on the ignorance of the people which is often exploited by fraudsters. These ignorant people in most cases ignorantly help the fraudsters to go through the control procedures" (B5)

Some organisations have also combined the procedural checks with the use of computer software and security systems for a more effective fight against online fraud. E.g. anti-viruses software, unauthorized access checks, CCTV, physical security check.

"Our strategy has been to always confirm the origin and authenticity of every transaction and procedural process through the vigilant eyes of our well

trained staff, and the power of our modern software and computer gadgets" (B16)

"Every organisation has a way of securing their assets and database; we have technological gadgets, software programs and procedural controls" (B13)

5.3.1.3 Complex / Cumbersome Operations

The installation of technological measures and procedural controls, however, presented an issue highlighted by some participants. These measures elongated the process and made it complex, while some customers found it cumbersome to follow through. The security questions, secret codes and passwords that have to be dealt with have been a source of concern to most customers, who often are not able to remember the answers required for the transactions to be processed.

"Most banks have installed gadgets and computer software to check online fraud which may be working effectively but the checking process it makes you go through is cumbersome and takes a long time" (B2)

"The security checks in place is for the good of our customers, it's unfortunate that they have to go through the rigors of the checks of which most have complained of. But it is like you putting a wall and a gate around the house and anytime you want to enter the house, your own house, you have to use the keys you must have kept in safe place to open the gate" (B1)

The findings showed that this issue has been a setback for most customers particularly the less educated and computer illiterates. Many have refused to use any online banking services offered by the banks.

"Most of our customers have complained about the complexity of the checks and some have even withdrawn from the services, but we are trying to simplify the procedures while maintaining the effectiveness of the security checks which we cannot compromise" (B21)

However, most participants agree that the complaints of the complexity of the procedural controls may be avoided if adequate training and proper education of the staff of the banks and their customers/public were made before, during and after the implementation of the control measures. This also highlights the importance and necessity of staff training, customer education and creation of necessary awareness of the countermeasures.

> "The lack of adequate information makes it difficult for the customers to understand and follow the new procedures, we have instituted some training and educative programmes to create the necessary awareness but it seems we have to do more to make it more effective" (B15)

5.3.1.4 Ignorance / Vigilance

Another major issue highlighted is that, in spite of the technological controls and procedural checks, online fraud is still on the increase due to the ignorance of most customers and online users. Most customers ignorantly aid and facilitate online fraud, which easily passes the controls and checks.

"A lot however depends on the ignorance of the people which is often exploited by fraudsters. These ignorant people in most cases ignorantly help the fraudsters to go through the control procedures" (B9)

The findings also showed that, apart from the ignorance of the customers, fraudsters have also exploited the carelessness of some staff.

"We have also discovered that because of the high level of security provision of our systems, fraudsters have sometimes taken advantage of the carelessness and lack of experience of mostly newly recruited bank staffs. In one or two occasions, newly recruited staff has been deceived to disclose some vital customer' details … in some other occasions dubious and questionable transactions have passed through the security checks unnoticed by some bank staff" (B14)

This experience has highlighted the need for vigilance and an understanding of the system by everyone concerned, particularly the staff of the banks.

"The watchful eyes of the staff and the vigilance of the customers also play important roles in preventing online crime" (B23)

"As a private individual the only way to prevent or detect online fraud is simply to be vigilant, always confirm origin and authenticity of every transaction, and update knowledge of computers and its modern use" (B18)

5.3.2 Control Focus

The findings showed that there are different security concerns identified by organisations that informed their interests and decisions on the technological measures put in place to fight online fraud and other related computer crimes.

5.3.2.1 Abuse / Unlawful Use of Computing Resources

The protection of their computing resources and prevention of unauthorised access were of high priority, followed by the protection of customers' data and illegal online activities. These influenced the technological controls and other checks introduced in the organisations. Most participants agreed that the protection of their computing resources and preventing unauthorised access should prevent all other computer related crimes. They therefore believe that all efforts should be focused on keeping computing facilities safely protected.

"Yes we have technological systems to mainly check against unauthorised access to our computing resources but unfortunately our focus has not been on online fraud which is usually associated with e-commerce. We believe the organisations involved in that should come up with systems to protect their customers from such online fraud" (B1)

"The focus of technological measures is to prevent the abuse of computer resources or use the facilities for unlawful purposes" (B12)

5.3.2.2 Protecting the Confidential Information of Customers

Other participants, however, suggested that, although keeping computing facilities safe is necessary, protecting customers' interests is more important. They argued that keeping the computing facilities safe is primarily in the interest of the organisation, but the concern and focus should be ,alongside the money and the protection of customers' identity .

"Our focus is to ensure that our customers do not fall prey to fraudsters" (B26)

"Our main focus is therefore to protect customers' confidential information and keep the trust of our customers who can on the other hand deal with issues of identity theft or any other online fraud on their own" (B9)

The findings also showed that the increasing wave of online fraud in the country has changed the focus of technological security to identifying and preventing online fraud activities.

"The technology is there for us to use and make life easy for us and the people that put their trust on us. We are aware of online deception, identity theft and the like, therefore our use of the technology is to prevent such activities and whenever any attempt is made the system should be able to promptly detect and flag it for investigation and arrest. But because we do not have the power to arrest and prosecute, we have to bring in the law enforcement who takes over from there. But again the activities of the law enforcements have not

been encouraging, nothing fantastic so far from deterring and discouraging others from such acts" (B17)

Others have the opinion that using technology to the optimum in checking both access to computing resources and protection is in the customers' interests.

"We can only use technological means to protect our technology and its effective use ...we have access controls both physical and software controls and other gadgets to monitor movements and activities of people using our systems or those around the resources" (B24)

5.3.2.3 Illegal online activities

Most participants also highlighted the efforts of most organisations, particularly government institutions, to monitor online activities aimed at tracking the use of illegal websites and the use of the Internet for illegal activities. This activity is not, however, focused on preventing online fraud, but on ensuring that people do not have access to government-banned websites or be involved in anti-religious / social activities such as pornography.

"The focus has been to prevent illegal activities online and the improper use of the Internet" (B6)

"The main focus of our controls is to monitor access to our system and Internet operations to enable us prevent illegal activities online" (B2)

However, this concern and focus has been useful in online fraud detection and the fight against online fraud and other illegal use of the computer to commit

crime. This service has been used in some cases to track down fraudsters when incidences of online frauds are reported.

5.3.3 Relevance and Adequacy of Measures

Participants also highlighted the issues of the relevance and adequacy of the technological measures in place. The issues raised included how safe and trustworthy the measures are, the role of the customers in the operation of the measures and making them effective, and the necessary regular updates needed to sustain the effectiveness of the measures.

5.3.3.1 Safety and Trust worthy

Most participants agreed that, considering the situation in the country, the present measures taken in combination with technological controls and procedural checks, are good enough for whatever focus or concern organisations may have. Some pointed out that the safety and adequacy of the measures have increased the confidence of the customers and enhanced their trust in the ability of the banks to protect their interests.

"I believe the measures are adequate enough because some of my friends consider the checks as safe and trust worthy, this has also encouraged some of my friends to participate in online banking and e-commerce offered, some are however discouraged because of the long routine of checks which is designed to deter potential fraudsters" (B13)

"We have made adequate arrangements and put some guidelines in place to deter fraud in our system. It is also easy for our system to pick any attempt of fraud in whatever means used" (B6)

However, some participants are of the opinion that the measures are not fool proof, but require constant monitoring and improvement.

"There are no safe and tight technological securities that cannot be cracked, so therefore we always strive to constantly update the system" (B4)

5.3.3.2 Involvement of the Customers

Participants also agreed that the relevance and adequacy of the measures in place cannot be complete without the active positive participation of the staff, as well as the banks customers. The involvement of the customers is seen as vital to the effectiveness of the measures.

"We feel the technological measures in place coupled with the strict religious stand of the bank have worked well both for the bank and the customers. We can boldly say they are adequate for now" (B9)

"A lot still need to be done in many areas, for instance the business people have to be properly instructed and made to be aware of the tactics of online fraudsters, people caught in the act or customers found to be colluding with fraudsters should also be reprimanded to stop others" (B15)

The study highlights the importance of customers knowing the measures put in place to protect them. It also shows the importance of gaining the cooperation of the customers and providing a platform for ideas and concerns to be shared and discussed. The bank authorities should also keep customers informed of their up to date securities systems to combat the latest techniques used by the fraudsters.

5.3.3.3 Regular Updates Needed

Participants also acknowledged the need for regular updates to meet with the changing trends in technology and the situational challenges of online fraud in the country.

"Technology is changing and therefore the measures need to be updated to accommodate current trend" (B1)

"We understand the prevailing situation in the country and therefore strive to meet the demands of the times and peculiar circumstances of the situation" (B26)

However, participants also agree that the banks and other organisations have not responded appropriately and timely to the changing technologies and societal needs which may also have compounded the issues of the failures of the countermeasures.

"Our organisations may not be that current and up-to=date with the realities of the changing technologies and challenges of online fraud

which may be linked to the level of awareness of the staff and public and the focus of the organisation" (B16)

5.3.4 Theme Summary

The findings showed the efforts of organisations to put in place relevant technological measures, coupled with procedural controls and checks. These measures have varied purposes, but the majority are focused on protecting computer resources, while only a few focus on protecting online activities.

The findings also showed that the measures have become obstacles to most customers, who find it cumbersome to engage in online activities, because of the procedures and checks. It also showed that these measures alone may not be adequate to prevent and detect online fraud, but the vigilance of both staff and customers, and more importantly, the cooperation of the customers are very much required.

5.4 Regulations

This theme presented the issues and challenges relating to regulations in the country and the impact on the prevention and the combating of online fraud (Table 16). Three main issues and sub-themes that highlight the effectiveness of the regulations are types of regulations, focus of the regulations and impact of the regulations.

Theme	Sub-Themes	Codes
Regulations	**Types of regulations**	Government regulations/laws In-house rules and guidelines
	Focus of the regulations	Internet monitoring Operational guidelines
	Impact of the regulations	Lack of awareness Lack of focus and purpose

Table 9 Regulation theme

5.4.1 Types of Regulation

Most participants agreed that the lack of appropriate and specific rules and regulations guiding online transactions in business may be the major loophole facilitating online fraud in the country. There are government rules and regulations guiding internet operations such as publications of pornographic materials, terrorist activities etc. but these rules are silent on the rights and privileges of the customers. Banks and other institutions have also formulated rules and regulations to guide their activities.

5.4.1.1 Government Regulations / Laws

The main concerns raised related to the inability of the government to establish a platform on which to build appropriate rules and regulations and acknowledge and stipulate the rights and privileges of the consumers and define what is an abuse of rights.

"There is no specific regulation that guides or protects the customers against online fraud, at least none that I know of. This makes it difficult to call

online fraud a crime that has to be controlled; most organisations have internal procedures and regulations for their customers designed to fight fraud" (B2)

Most participants expect the government to set the stage for online transactions, with clearly defined roles and responsibilities, but this is lacking.

"As a private citizen I rely on the government's ability and goodwill to protect their citizens by enacting adequate laws guiding the operations of online business transactions but unfortunately these laws are lacking or present ones are inadequate and not known by many" (B5)

"We totally depend on the government's regulations and sometimes on the regulations and procedures put in place by organisations we transact with, however, the government's regulations or organisational procedures need to be made clearer and accessible to every interested persons or groups" (B6)

However, there are indications that the government is putting in place some guidelines to support e-commerce and other online activities that would rather aim at monitoring Internet usage in the country.

"The government has provided regulations as guidelines to the use and operations of internet services by organisations and individuals, however, these regulations have not been given adequate publicity as most members of the public are still ignorant of how things are done" (B9)

"The regulations cover the use and operations of internet services and all kinds of transactions in e-governance and e-commerce ... the regulations provide necessary guidelines to business organisations and internet service providers ... it also stipulates charges and punishments to erring customers/organisations" (B5)

5.4.1.2 In-house Rules and Guidelines

Acknowledging the importance of rules and regulations in online operations, but unfortunately as the government could not provide guiding principles and rules on online transactions and fraud, most organisations had to define the rules for both customers and staff.

"Although we are guided by government regulations which are not all that specific on online fraud, we have our own internal rules and regulations which guide our operations and these rules are made public for everyone to see, both staff and the customers" (B24)

"We believe we have to set our own house in order and ensure that our staff and customers are dissuaded from engaging in any fraudulent activity within or outside the bank. Our staffs in particular know the consequences of such actions as published in organisation's newsletter, and so far, everyone seem to be complying" (B18)

"We have internal rules and regulations made known to every staff and customers on how to handle and protect the electronic cards and devices in their control at all times, logging in and out procedures are emphasised, the

penalties for voiding such rules are also stipulated to make known our stand. This is to serve as disincentives and as deterrence to potential criminals" (B7)

The rules and regulations are also designed in conformity with international standards, to bring uniformity to online operations, which are aimed at facilitating the fight against online fraud.

"Based on the reports from International banking bodies on the nature and mode of online fraud, we have designed procedural guidelines to serve as rules and conditions allowing our customers to participate in our online banking systems" (B4)

"Circumventing the internal rules is an offence and we have had some experiences where staff at the bank connive and collude with fraudsters, and actions taken against such staff are usually published in the organisation's bulletin/magazine to deter others" (B1)

Participants also agree that issues of criminally minded staff should be checked by putting up stringent controls in employment of bank staffs. Regulatory bodies and law enforcement agencies may need to help scrutinise potential employees.

"Our regulatory agencies can help us to know the background of our potential staff and customers"

The carelessness of the staff is also attributed to the quality of staff and training given to the staff. The quality of the staff relates to competencies, qualifications

and background experiences, while the quality of training relates to the adequacy of the training, relevance and frequency of training.

"Most of our staffs are graduates although not in banking or business, but with a minimum four years' experience. Our training schemes start with an induction and regular updates in different sections of the banking industry. However, as we experience new cases of online fraud, our training need to be focused on the types of online fraud and ways of stopping them" (B15)

5.4.2 Focus of the Regulations

Most of the participants agree that the regulations are meant to provide a level playing field for all participants involved in online transactions, guiding their activities and protecting their rights. The picture, however, shows a different focus when it comes to government rules.

5.4.2.1 Internet Monitoring

The concern raised is that the government's regulations are focused on monitoring Internet usage, and therefore they have not done much to provide the rules and the platform to effectively deter, prevent and detect fraud.

"Government's regulations are mostly to protect computer resources and regulate the use of the Internet only for approved activities; I believe the government will have to do more by focusing on online fraud to make the fight against online fraud a success" (B13)

"As far as I am concerned, the available government regulations are focused on monitoring the use of the Internet for anti-religious activities such as pornography ... not much is done about preventing and penalising offenders. The focus should now be the online crime and electronic commerce" (B22)

However, the rules and regulations formulated by private organisations, such as the banks, have focused more on deterring, preventing and detecting fraud, with little success.

"We have not seen government regulation helping out to prevent or fight online fraud in any way; all we have achieved so far have been through our in-house regulations and procedures" (B25)

"The government rules and regulations are scanty and do not cover all the areas of e-commerce to protect the operators, they are simply inadequate" (B14)

Another major concern raised is the opinion that, for the internal rules and regulations to be effective in deterring and eradicating online fraud, they must be anchored on clear government laws binding on all.

"But whatever rules and regulations we make in our organisation can only be based on the laws of the land … this situation where the law of the land is not strong on deterring and preventing online fraud, is a limiting factor" (B7)

Participants therefore agree that the influence of the government and the society may have to be used to help give a backup cover to the countermeasures adopted by the banks.

> "*The government needs to come to our rescue in giving us necessary cover in legislation to make our countermeasures effective"*

5.4.2.2 Operational Guidelines

Another major focus of both government regulations and in-house regulations is the provision of operating guidelines for individual users and organisations.

> *"The regulations cover the use and operations of internet services and all kinds of transactions in e-governance and e-commerce … the regulations provide necessary guidelines to business organisations and internet service providers ….it also stipulates charges and punishments to erring customers/organisations" (B8)*

It is noted that these guidelines have helped in putting in place a structure to enhance the prevention and detection of fraud.

> *"The regulations have been able to provide the baseline for other infrastructural and institutional facilities to collectively prevent, detect and fight online fraud" (B3)*

The result of the setting up of the regulations was the development of technological infrastructures, which further enhanced the effective prevention of online fraud.

"The regulations coupled with the technological infrastructures are keeping check on fraudulent practices to detect and prevent" (B7)

Another issue that shaped the focus of the operating guidelines is Islamic banking rules. This is claimed to have contributed to the success in the fight against online fraud.

"The government has also been very supportive using the guidance of the Islamic law in banking which has contributed to the success recorded against fraudulent activities" (B20).

5.4.3 Impact of the Regulations

Many concerns were raised regarding the workability and the impact of existing rules and regulations on deterring, preventing and detecting online fraud in the country. Most participants agreed that the existing rules and regulations on internet use and e-commerce have not had any impact on the fight against online fraud. This may be due to lack of understanding and awareness of the circumstances of online crime in the country. It may also be due to lack of focus and purpose of the regulations.

5.4.3.1 Lack of Understanding and Awareness

Participants agreed that the government agencies responsible for internet operations and most banks might not have completely understood the complexities and intricacies of online fraud in the country.

"There are no regulations in place for now to control online fraud ... the government has to first of all understand the situation and then come up with suitable regulations" (B20)

"The government is still studying the industry and the scope and breadth of online fraud in the country, the regulations in place at the moment may not be adequate ... but modifications and upgrades are constantly made whenever necessary" (B4)

Online fraud is considered to be in its infancy and relatively new in the country, and, as such, most regulations are still inadequate to deal with it.

"To the best of our ability the regulations in our organisation are adequate to fight online fraud in its infancy in the country ... as the sophistication of the crime increases we shall also modify and update to meet up with the challenges" (B16)

"I believe with time specific regulations will be made to cover all aspects of online fraud" (B15)

Participants also highlighted the need for the government through its regulatory agencies to educate the general public on online fraud and the regulations defining the types of online fraud and prosecution process.

5.4.3.2 Lack of Focus and Purpose

Due to the lack of understanding of the circumstances of online fraud, the rules and regulations guiding online transactions aimed at protecting participants and preventing online fraud lacked focus and purpose.

"No the regulations may not be adequate as there is still a long way to go … but the government's resolve to combat all sorts of online fraud will leave no stone unturned … necessary regulations will be enacted" (B4)

"Our rules and regulations are serving the purpose for now but we still need the government regulations to back us up, and unfortunately we don't have such government regulations" (B12)

Due to the lack of focus and purpose and the low impact of the regulations, most participants are of the opinion that the right focus should be the prevention of fraud, with the use of appropriate technologies to back up any regulations. It is argued that regulations can only define anomalies and proscribe appropriate punishments aimed at deterring offenders, but they do not prevent fraud.

"Although we trust in the ability of the use of penalties to deter criminals, our focus however is not to allow them to operate at all, this we are doing by

bringing in technology to prevent and detect any attempt to defraud, this has really paid up for us" (B10)

Another glimmer of hope is the use of Islamic laws to help with the guidelines and regulations to fight online fraud. Participants agreed that this could give a new focus to the rules and regulations on online activities.

"We have faith in the Islamic law which discourages fraudulent acts such as online fraud there must be a way of using the Islamic laws to help fight online fraud" (B7)

5.4.4 Theme Summary

The regulations governing online activities are highlighted as very important in the prevention of online fraud. The findings show two types of regulations, government and organisational rules, with different foci and purposes. The focus of most of the regulations is on monitoring internet operations and operational guidelines, which are also regarded as very important. However, the regulations have not been able to make much impact, owing to lack of awareness, lack of purpose or non-existence.

5.5 Enforcement

The enforcement of existing rules and regulations and bringing criminal individuals and organisations to justice were considered a major handicap and impediment to the prevention of online fraud in in Saudi Arabia (Table 17). The system of prosecuting offenders was seen in the light of the passive nature of enforcement, socio-cultural and infrastructural handicaps and the lack of

experience of the enforcement agencies. The state of preparedness of the agencies was also highlighted in terms of their training and infrastructural base. The two sub-themes presented here are the prosecution of offenders and preparedness of agencies.

Theme	Sub-Themes	Codes
Enforcement	**Prosecution of offenders**	Passive enforcement Socio-cultural and infrastructural handicaps Lack of knowledge/experience
	Preparedness of agencies	Training Infrastructural base

Table 10 Enforcement theme

5.5.1 Prosecution of Offenders

Participants had the opinion that enforcement is a function of the level and effectiveness of the prosecution of offenders. Moreover, successful prosecution depended on the activities of the enforcement agencies, the infrastructures available and their experience.

5.5.1.1 Passive Enforcement

It is reported that, in spite of the increase in the rate of online fraud in the country, the rate of prosecution of online fraud offenders is very low. Participants agreed that the enforcement agencies had been very passive and nonchalant. No serious effort had been made to nip in the bud the rising rate of online fraud.

"I have not seen any activity of law enforcements regarding online fraud; they have been very passive about online fraud, making people to believe online fraud is no crime or that there has never been any online fraud. This calls for the publishing of all prosecuted cases and convicted offenders to deter others" (B10)

"I have never heard of any online fraud case brought to the court or of any online fraudster reprimanded. Neither the government nor organisations have been able to bring any online fraudster to judgement. This non action by the law agencies could even encourage online fraud rather than serving as deterrence to would-be criminals" (B14)

This inaction may be due to some of the other issues highlighted (infrastructural handicaps and lack of knowledge). Nevertheless, the seriousness of the agencies about combatting the menace of online fraud has also been questioned.

"There has not been any sign of seriousness of purpose on the part of law enforcements, no public statements or policies to warn unsuspecting citizens and to show their preparedness to protect the people" (B7)

"There is no indication of seriousness on the part of law enforcement agents to effectively handle online fraud. No assurance of any kind. This could be due to their lack of awareness, knowledge and poor educational background" (B6)

5.5.1.2 Socio-Cultural and Infrastructural Handicaps

Participants agreed that enforcement agencies were much handicapped in the prosecution of offenders, owing to the nature of online fraud. Evidence is required for prosecution.

"Online fraud is a technological crime and it can only take technology to solve it, it is usually said that it takes only a thief to catch a thief" (B23)

The faith in Islamic law and the belief that justice would be enacted in one way or another may also have contributed to the nonchalant attitude of both the agencies and the victims, who may feel reluctant to press charges.

"The Islamic law is very clear on ways to bring erring people to justice, and this has been very effective" (B11)

"We have faith in the Islamic law which discourages fraudulent acts such as online fraud" (B3)

Participants thus agree that effective countermeasures and the prosecution of online fraud could be based on the effective use of the sociocultural environment. Shari laws and religious institutions may play vital roles in the prosecution of offenders.

"The strong faith in Islamic laws could be used to deter potential criminals and also in the prosecution of offenders"

The lack of adequate infrastructures was also highlighted as a major limiting factor in the prosecution of offenders.

"So far the prosecution rate has not been encouraging due to some lack of infrastructures both technically and legally…you need technological based evidence to successfully prosecute and you also need laws to prosecute offenders … these things are somehow lacking to an extent" (B2)

"Technology has advanced in many ways and may be difficult to successfully prosecute and convict online fraudsters who use advanced technologies to hide and clear their tracks" (B4)

Another basic infrastructure element lacking is an adequate legal framework required to support effective prosecution of offenders. The existing laws are not very clear on the nature and types of offences relating to online fraud, and they do not give clear direction and guidelines to prosecutors.

"I have not seen anyone prosecuted even though the online crime rate is increasing daily…it is sad that the law enforcement agencies are handicapped to deal with the issue of online fraud without adequate law and regulations for backups" (B7)

Most of the participants highlight the need for the government to legalise the use of electronic and digital signatures as evidences in legal proceedings and to help procure such technological equipment to prosecute offenders.

5.5.1.3 Lack of Knowledge / Experience

The findings also showed the obvious lack of knowledge and experience of the enforcement agencies and agents involved in the prosecution of offenders.

"Reporting my online fraud experiences was meaningless and valuable time and resources wasted. They simply had no clue of what to do and tried to blame me for what happened. I believe this is perhaps due to their lack of awareness, exposure and experience in handling such cases" (B19)

The opinion was that online fraud is new and relatively unknown to many agents. Exposure of the agencies to such fraudulent practices may therefore be needed.

"Online fraud is alien to our culture and society; the technologies used are also strange to us in this part of our world" (B25).

5.5.2 Preparedness of Agencies

The findings also highlighted the efforts of the agencies in setting up the right atmosphere to effectively carry out their functions. The efforts included the training of staff to give them the necessary skills and knowledge, and the provision of an infrastructural base to enhance their work.

5.5.2.1 Training

The indication was that the agencies had not shown any seriousness in their fight against online fraud in the country. It also exposed their lack of preparedness and inadequacy in enforcing laws and eradicating the country of online fraudsters.

"There has not been any sign of seriousness of purpose on the part of law enforcements, no public statements or policies to warn unsuspecting citizens and to show their preparedness to protect the people" (B6)

"No idea whatsoever about the readiness of the law enforcement agencies … although from time to time some announcements are made to inform the public on fraudulent activities discovered" (B23)

Participants agreed that they may have been responsible for the lack of seriousness and the law enforcement agencies' lack of preparation in the fight against online fraud, because of lack of knowledge and skills. Training and exposure is therefore suggested to bridge that gap.

"I don't trust on the ability of law enforcements to handle issues of online fraud that seem to be too hard for them to crack" (B21)

"The low level of awareness and the lack of adequate training is clearly demonstrated in the way the agencies have handled the prosecution of online fraud so far, it is evident that training is required urgently" (B18)

The government's efforts in providing the necessary training are also highlighted as a priority to remedy the situation.

"The government is introducing training to update the operational skills of the staff and also introducing new technological infrastructures to equip the agencies handle technologically based crimes" (B6)

"We have taken some training to help us be in tune with the demands of technological crime such as online fraud; this has so far equipped us to handle effectively new cases that have been brought to our attention. Our confidence and competence is growing by the day" (B7)

5.5.2.2 Infrastructural Base

The lack of a necessary infrastructural base is highlighted as one of the issues limiting the fight against online fraud. The government law and enforcement agencies are not adequately technologically empowered to deal with cases of advanced online fraud.

"I don't trust on the ability of law enforcements to handle issues of online fraud that seem to be too hard for them to crack" (B15)

The findings also highlight the government's actions in equipping the agencies with state-of-the art technologies.

"The government has initiated some training program for law enforcement agencies to update their knowledge on current technologies … new technological infrastructures are also put in place to help in the detection of online fraud … this is to equip the agencies both in skills and facilitates to handle cases of online fraud" (B9)

5.5.3 Theme Summary

The enforcement of rules as regards prosecuting offenders has been minimal and passive. There is a nonchalant attitude on the part of the agencies to carry out their duties effectively, due to some legal and technological limitations, as well as their lack of knowledge and experience. The efforts of the government to train and equip the agencies are also acknowledged.

5.6. Summary

The chapter presented the qualitative data using the themes identified from the data set. The findings showed that frequency of occurrence is increasing due to the increased activities of e-commerce; meanwhile the level of awareness is low, owing to lack of knowledge, training, lack of government sensitisation and the religious inclinations of the population. The findings also confirm the efforts of the organisations to put in place countermeasures using various technological measures, coupled with procedural controls and checks. However, the majority of these countermeasures are focused on protecting computer resources, while only a few are focused on protecting online activities. The measures are also becoming obstacles to most customers, who find it cumbersome to engage in online activities, because of procedures and

checks. The findings also show two types of regulation: government and organisational rules, with different foci and purpose. They mostly focused on the monitoring of Internet operations and operational guidelines. The enforcement of rules in the light of prosecuting offenders has also been minimal and passive.

CHAPTER 6

6. DISCUSSION

6.1 Introduction

The last chapter five presented qualitative analyses of the different sets of the data collected. The analysis highlighted factors surrounding perceptions, awareness and familiarity with the different types of common online fraud, frequency of occurrence and the different preventive measures adopted, such as technological application, economic and legal / regulative measures. The qualitative analysis also presented a deeper insight into the perceptions, technological measures, regulations and enforcement activities of staff in banking organisations, and those who influence online fraud activities. This chapter brings together these issues and activities and discusses how they have affected online fraud deterrence, prevention, detection and remedy, individually and collectively. This chapter also assembles the main points of the research and summarises the findings which highlighted the main themes about online fraud and countermeasures in Saudi Arabia.

6.2 Perceptions of Staff, Employees and the General Public

The data highlighted the breakdown in the position of people in terms of viewing online fraud as a criminal activity, and goes deeper to show the interpretation and the meaning of online fraud as perceived by the participants. The data analysis indicates that most of the participants viewed online fraud as

a criminal activity carried out using computers and the Internet, but few viewed it as a social act, while very few did not see it as a crime, but blamed it on people's social lifestyle and greed. The participants who viewed it as a criminal activity saw the nature of the online fraud and its scope and range in the use of the Internet through any medium, such as mobile phones, ATMs and so forth. On the other hand, participants who did not see online fraud as a crime considered the nature of online fraud as a smartness born out of greed for self-satisfaction. The qualitative data analysis therefore concludes that online fraud is a criminal activity but also emphasises on the importance on the influence of participants' cultural, societal and educational background on the meanings attached to online fraud (Silver and Miller 2004; Adler and Kwon 2002).

People's mind-sets are based on their moral inclinations, which form the background to their differing views, and may be seen as major issues affecting deterrence, prevention and the detection and remedy of online fraud (Cornish and Clarke 1986). The intention and motives of a person to carry out online fraud were highlighted, and these were significant issues in deterrence activities. The highlighted view that online fraud is technology-based and a computer-engineered activity also form a major issue in prevention and detection activities. The emphasis on the position of law and the government emerged in the clear classification of online fraud as a criminal activity, and this affected perceptions, playing a significant role in the deterrence, prevention and remedy to online fraud.

The implication of the perception as analysed is threefold, affecting the three pillars of the fraud triangle (Cendrowski *et al*., 2007).

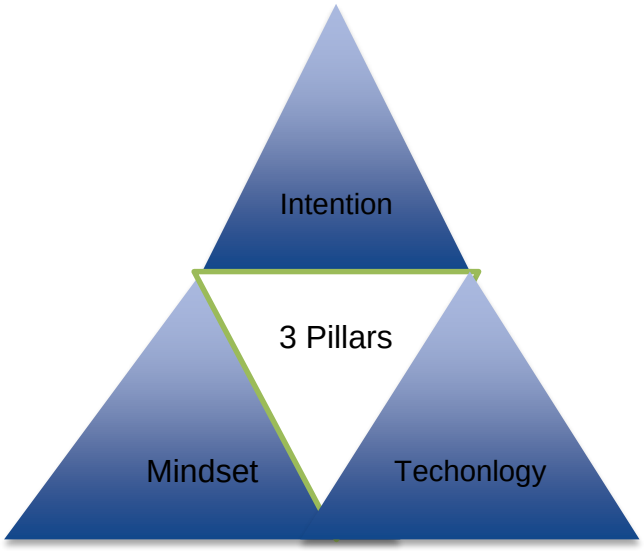


Figure 5 Triangle pillars

The first is the intention and motive of the perpetrator, which can be positively manipulated through socio-cultural training to help in fraud deterrence. The second implication is the mind-set of the fraud perpetrator, which rationalises and drives the wrongful act. This can be altered positively through training and sensitisation to enhance effective fraud deterrence. The third implication is that the view that online fraud is technology-based and a computer-engineered activity (Majad, 2008) suggests that the technology used in business creates an opportunity, such as control lapses or weaknesses that allow the fraud. A periodic examination of the control system therefore needs to be carried out, to enhance the effective prevention and detection of fraud. Furthermore, the influence of a lack of clear laws on perceptions of committing the crime, such introducing punishment implies the need for clear and specific laws about

online fraud to enhance better deterrence, prevention, detection and remedy of online fraud.

6.3 Awareness and Occurrence

The analyses confirmed the important role of awareness in online fraud activities and the challenges posed for deterrence, prevention, detection and remedy of online fraud. It is pertinent to note that a low level of awareness is mainly due to a lack of knowledge among bank officials and government regulators. Their level of education and training, religious inclinations and lack of government sensitisation were also contributory factors to the low level of awareness and that because of the ego of banks officials and managers in the banks in Saudi Arabia of having an adequate countermeasures as its indicated in section 5.2. These are sensitive issues and activities that have not been understood by the banks and the government in the country that could have determined the actions of the bankers in altering how the criminals perceive online fraud (Kelvin Cgilton, 2009).

Another pertinent issue highlighted by the analysis is that, there is a low level of awareness among bank officials in Saud Arabia towards the issue of online fraud. The findings revealed that, due to fear, lack of trust in banks and lack of clear laws defining online fraud, most end users failed to report occurrences of online fraud to the banks or law enforcement agencies as is apparent from section 5.2.2.3.

Most of the online frauds experienced by the public are also e-commerce related and therefore not generally reported. This is due to the lack of awareness of the law enforcement bodies in Saudi Arabia towards the issue of online fraud and such crime. The implication is that, the public left without support from the banks and the government, who are lacking awareness or are not familiar with the type of online fraud experienced. This has a negative impact on deterrence and the prevention of online fraud, which requires familiarity and sensitisation to create the necessary awareness (Gartner Group, 2009).

Furthermore, the effectiveness of the introduction of anti-cybercrime law in 2007 has been limited due to the lack of awareness for such legislations, Which makes people reluctant to report such crime in order to combat it (Elnaim , 2013).

The banks are more familiar with computer hacking, phishing attacks and other potential threats to their computer resources, and are therefore more focused on protecting their resources, and the prevention and detection of computer crimes. This also has serious implications such as proactive measurements for deterrence, prevention, detection and remedy. Moreover, the findings indicate that the banking staff's insensitivity to online fraud is largely due to their educational background, lack of necessary training and skills, and the vision and focus of the management (Aransiola, 2011). The banks are not familiar with online fraud and its tricks and therefore do not have enough experience to guide and advise their customers. All of these are required ingredients for

successful deterrence, prevention, detection and remedy. (Whitman, 2004) Moreover, as indicated by the findings, poor security awareness, for example lack of expertise of online fraud techniques within the banks, is a major issue in the rise in online fraud, which needs to be addressed.

The high frequency of occurrence of online fraud, however, has also influenced increased awareness for those who faced it, which has necessitated some positive moves by the banks to prevent further occurrences. Training programmes and other awareness creation programmes, coupled with the establishment of some preventive measures of control, are being instituted by the banks. This indicates the banks' concern and need to combat the increasing threat of rising online fraud. The success of these measures, as indicated by the findings, depends on the focus and purpose of the measures, which were mainly detection to a large extent with most banks, and prevention to a lesser extent. The overall success of the measures in the whole picture of deterrence, prevention, detection and remedy of online fraud is however minimal and dubious.

The highlights of this theme have several implications. Adequate training and sensitisation to create the necessary awareness should back up the government's desire and push for e-commerce activities, which have increased online activities. A customer-friendly reporting status / system with assurance of confidentiality is also needed to encourage customers to freely report all occurrences of fraud to the appropriate authorities for prompt action. The banks also need to shift focus to preventive measures against online fraud.

6.4 Preventive Measures Adopted

The analysis also highlighted the most common types of online fraud in the country (phishing followed by identity theft, online investment fraud, online auction fraud and advance fee fraud). However, although phishing attack is the single most common crime representing 64%, the other types of online fraud, account for 36%. Unfortunately, however, the focus of the preventive measures in most banks has been on combatting phishing attacks, while the other types of fraud are regarded as less threatening and are not given as much attention. This calls for a strategic change and an emphasis on online fraud and its causal factors.

The implication is that the situation that creates the opportunity allowing the fraud to occur is left unchecked. It is argued that an analysis of the conditions and procedures affecting fraud enablers would be an effective preventive measure to enhance fraud deterrence (Cendrowski *et al*., 2007). Unfortunately, the installation of the preventive measures has brought a complexity to operational procedures, which inconveniences the customers. Customers' ignorance and bank staff's lack of vigilance or lack of skill have also been noted to have created opportunities for online fraud. The vigilance and understanding of the system by everyone concerned, particularly the bank staff and their customers, is urgently required through regular training and workshops. This would enhance both the organisational, procedural and cultural orientation needed for effective fraud deterrence (Cendrowski *et al*., 2007).

6.5 Online Fraud Detection

Organisations agree on the use of technological devices and applications, seen as the most reliable in fighting online fraud, which are technology-based and enhanced by current technologies. Organisations have therefore installed different technological infrastructures to facilitate the monitoring and detection of online fraud. However, the recent fraud of 45 million US dollars from Gulf Banks by a gang of criminals who hacked into the banks' system using stolen debit card details suggests the inadequacy of technological gadgets and questions electronic protection procedures (Alrabiya, 2013). Although Saudi Arabia holds one of the best protection services for electronic bank systems amongst Arab countries, full protection over the Internet may not be secured. An IT security expert opines that important aspects of electronic protection are often overlooked in the electronic system itself. There may need to be monitor online systems for any threats by hackers. This corroborates the argument that fraud detection involves a review of historical transactions, to identify indicators of non-conforming transactions (Cendrowski *et al*., 2007).

The findings show that most banks now see the protection of customers' information as a major priority, to ensure that customers do not fall prey to fraudsters. The technology installed is to monitor and promptly identify, detect and flag activities, such as online deception and identity theft for investigation and arrest. Using installed technology to the optimum in checking both access to computing resources and the protection of customers' interests is therefore a necessity. However, making a success of it may also depend on the cooperation of the customers and the staff.

The customers may have to ensure that their debit cards and other confidential passwords are kept safe and secured, and to report any loss or suspicion. The issue of customers knowing the measures and cooperating with the bank is very important, and raises some concerns with the authorities. The managing director at a Saudi technology investment company stated that electronic fraud occurs most of the time because of users' mistakes that needed to be addressed. This again implies a re-orientation of the customers in being security conscious as a requirement of the new system. The existing socio-cultural norms, which influence customers' orientation, may have to be adapted.

The involvement and active participation of the staff and the organisational culture is also vital to the success of the technological measures used in fraud detection. Staff training in the new requirements of the procedural change and technological measures may have to become regular to establish a new culture in the bank. This would provide staff with the necessary skills, exposure and experience to address the issues that lack of skills and confidence of staff has contributed to the experience of online fraud. This implies changes in the organisational practices of the banks to reflect and adapt to the demands of technological changes.

Furthermore, the changing trend in technology and the situational challenges of online fraud require that the measures need to be updated to accommodate the current trend. This implies that organisations must understand the prevailing

situation in the country and take adequate measures to meet the demands of the times and the peculiar circumstances of the situation. The safety and adequacy of the measures need to be ensured to increase the confidence of the customers and enhance their trust in the ability of the banks to protect their interests. This implies constant monitoring, improvement and updates to the system.

6.6 Remedy of Online Fraud and Enforcement

The literature notes that the measures aimed at remedies that seek restitution, and most importantly to re-enforce the deterrence of others, are gaining focus and need to be in place for effective deterrence, prevention and detection of online fraud (Cheng *et al*., 1997). Remedy measures are to be aimed at giving punishments for any fraudulent act (Kotulic & Clark, 2004). The findings suggest that, in spite of the increase in the rate of online fraud, the rate of prosecution for online fraud offenders is very low. This implies low or lack of remedy activities on the part of the banks and other regulating authorities, as noted by some participants. The implication of this passivity is that it makes people believe that online fraud is not a crime, or that there has never been any online fraud. Thus, it encourages, rather than discourages, the continuation of the wrongful acts of online fraud.

The passivity of the concerned authorities has also been blamed on socio-cultural and infrastructural handicaps, as well as lack of knowledge / experience and the preparedness of the concerned authorities. The passive and nonchalant attitude of the concerned authorities shows unfavourable

organisational culture and practices, which have much influence on the fight against online fraud. Blaming socio-cultural and infrastructural handicaps shows the influence of the environment on organisational culture and practices. The lack of knowledge / experience also shows the level of capacity and inefficiencies of the organisations, again reflecting organisational practices. The preparedness of the concerned authorities, however, shows the impact of the industrial and socio-cultural environment.

The socio cultural handicaps highlight issues of the social and religious norms and the lack of regulatory laws to create remedy activities. Specific laws and technology-based evidence are needed to successfully prosecute offenders. Furthermore, fraudsters need to hide and clear their tracks; therefore bank staff use advanced technologies, and other prosecuting / investigating officers need to be skilled and trained in technology. The findings show that this required skill and training is lacking and has affected the giving of punishment or reward for any fraudulent act. The implication is that the preparedness of officers is based on and may be guaranteed by the provision of training and an adequate infrastructural base.

6.7 Regulations

This platform is also required to guide the operating banks in designing their in-house rules and regulations. This dependence again shows the impact of the environment on organisational practices. In the absence of appropriate government laws, operating banks have devised procedural guidelines to serve as rules and conditions allowing staff and customers to participate in the online

banking systems. Most operating banks have internal rules and regulations that are made known to each member of staff and customers, stipulating how to handle and protect the electronic cards and devices in their control at all times, while emphasising logging in and out procedures, and the penalties for avoiding such rules. The internal rules are therefore set as deterrence to staff and create remedy measures, but may not be legally binding on customers if the law of the land does not provide the necessary backing. The focus of existing online transaction laws and guidelines and their impact on the effective fight against online fraud has also been questioned. Participants decried the focus of the laws on Internet usage monitoring, which has not done much to help deter, prevent, detect online fraud and penalise offenders.

6.8 Theoretical Reflections - General Deterrence Theory (GDT)

The four components of the general deterrence theory (deterrence, prevention, detection and remedy activities) in the study organisations were examined to see how these are systematically organised to impact online fraud in Saudi Arabia. Prevention activities also work to enhance detection activities, and remedy activities help in deterring others.

The activities of each component and the interrelationships of the components have a collective impact on combatting online fraud. The activities in each component and the relationships between the components therefore become very important in the success of the approach / theory. The theory therefore argues that the success of any effort or approach to combatting fraudulent activities depends on the activities of these four components, which must be

visibly seen to be in operation in the organisation. Some organisations may focus on only one or two of the components, such as prevention and detection, while being silent on the others.

The highlights of the findings show the different activities in some of the components and nil activities in others. This implies that some banks are focused more on some components, such as prevention and detection than others, such as deterrence and remedy. The focused components also have a few activities that are largely focused on other forms of computer crimes. This may have been responsible for the little success in some organisations and better success in others. This shows that the countermeasures are crime-centred approaches (Clarke, 1997).

The theory also suggests that there should be a systematic approach to the organisation and coordination of the components that are interrelated. For example, remedy is at the centre of the systematic approach; it serves as a corrective and punitive measure to a detected crime, aimed at deterring potential criminals. This implies that, without detection of crime, punitive measures cannot be applied to deter others. Deterrence activities such as awareness creation and training of staff may also enhance better prevention of crimes as people become more vigilant. A high detection rate may also mean that the preventive measures and the deterrence measures have failed. This shows the relationships between the components and the importance of the components working systematically together.

The theory therefore suggests proactive measures by using deterrence, prevention, detection and remedy activities to first create an environment or situation that deters people from committing fraud, and put in place measures to prevent fraud from occurring, but, if it occurs, to systematically detect the fraud with purposeful detection activities, and reprimand offenders. The certainty and severity of punishment may have to be made known to everyone, to influence potential offenders' perceptions of the net benefits of committing such a crime (Straub, 1990).

6.9 Reflection on Environmental Influences

These are the socio-cultural, industrial and organisational environments. However, although all three may directly affect countermeasure activities, the socio-cultural and industrial environments are also seen to have a more direct effect on the organisational environment, which in turn influences organisational practices and countermeasure activities.

6.9.1 Identified Activities, Issues and Concepts in the Proposed Model

6.9.1.1 Social Cultural Environment

The socio-cultural and religious environment of Saudi Arabia was seen to have much influence on the people, organisation, practices and the measures used to combat online fraud. The perception of the people and awareness of online fraud, which are seen to have a critical influence on deterrence, prevention, detection and remedy, are firmly grounded on socio-cultural norms and religious beliefs as highlighted by the participants in the data set. These

findings confirm the argument of social learning theories which suggest that the socialisation of the people and social bonding between them may influence criminal intentions (Hirschi, 1969; Burgess & Akers, 1966).

The implication therefore is that the socio-cultural environment can be used as a channel to positively provide counter measures to online fraud. Religious teachings and social norms could be tailored through regular adaptive teachings and social education in mosques and other social gatherings, to guide a positive perception of online fraud and create the necessary awareness of the evils of online fraud and consequences, which could serve as deterrence (Nolan et al. 2004; Adler 2001). Educational institutes through the secondary and tertiary schools could also be instrumental in providing needed knowledge in computing and electronic commerce for positive perception and awareness. Government and organisations could therefore carry out the following activities identified in the data set /analysis, through societies, clubs and educational institutions. The activities which are based on the recommendations of the participants and other observed practices in literature are as follows:

1. Religious teachings and sensitisation
2. Social sensitisation
3. Reiterating good social norms
4. Educational reforms
5. Integrating ICT in education

6.9.1.2 Industrial Sector Environment

The financial sector is seen as an important sector in the businesses of the people and in the economy of Saudi Arabia. The sector is full of activities,

financial inflows and outflows, and therefore attracts much attention from government, financial organisations and the public. The financial sector is thus perceived by potential criminals as a viable and good ground to perpetrate their criminal intentions. Clarke (1997) suggests that the incidence of crime is a function of the perceived costs, perceived benefits and degree of rationalisation.

The government's concern about the development of the sector is demonstrated in the efforts to simplify the financial process with the introduction of online banking, e-commerce and e-payment. Facilities were also provided to encourage business organisations to take full advantage of ICT potentials. This resulted in the proliferation of online devices and an increase in the online banking user base, most of whom were unaware and uneducated as to the dangers of online banking and the threats of online fraud. Financial organisations also intensified online banking and transaction activities, encouraging user participation and the introduction of procedural and facility changes without adequate public education.

The implication is that the demands of the sector continuously put pressure on the organisations in the sector and the government to modernise the sector for efficiency, cost effectiveness and to meet international standards. The demands include fast and immediate access to financial data / information, quicker and more secured financial transfers / payment and fast customer verification. The organisations and the government reacted to the demands without adequate training of staff, education of the customers and the general

public, appropriate local / customised procedures, clear guidelines, and rules and punishment for offenders. These were highlighted in chapter five as factors responsible for the lack of impact of the countermeasures implemented by the banks. Based on these highlights and suggestions from the participants to remove any obstacles and make the countermeasures more effective, the following activities are therefore required in the organisations and within the financial industry/environment for effective deterrence, prevention, detection and remedy of online fraud.

1. Staff training
2. Customer and general public education
3. Appropriate local / customised procedures
4. Clear guidelines, rules and punishment for offenders

6.9.1.3 Organisational Environment / Practices

The study confirms that organisational practices are more direct responses to the demands of the socio-cultural and industrial sector environments than changes in technological advancements. Religious beliefs and some social norms are major considerations in organisational practices. The demand for fast and immediate access to financial data / information, quicker and better secured financial transfer / payment and fast customer verification also guided the practice and operation of most organisations.

The study highlighted several organisational issues ranging from organisational transaction policies, recruitment and training policies, and technological infrastructures to human development policies. These issues were seen to have affected the impact of the countermeasures in the organisations. Activities

targeted at enhancing effective deterrence, prevention, detection and remedy of online fraud are therefore based on addressing these issues as follows:

1. Organisation policies
2. Hiring / recruitment policies
3. Strategic planning
4. Training and human resource development
5. Policy implementation

6.9.1.4 Deterrence Activities

The study confirms that deterrence activities aim to create awareness and inhibit fraud before it is carried out. Deterrence activities also help facilitate prevention activities by establishing necessary awareness of the crime, the rules and the consequences, for the operators of the system and the customers of the bank. The activities identified in the study and suggested by participants that could create impact in making the countermeasures more effective and successful are:

1. Incentives such as bonuses, loyalty awards, clean records, and so on.
2. Disincentives such as news bulletins about fraudulent activities.
3. Policies outlining what the organisation consider fraudulent activities and consequences.
4. Awareness creation using publicity, such as organisation websites, marketing slogans, and so on.
5. Training of the staff and customers in online banking transactions and potential threats.

6.9.1.5 Prevention Activities

Prevention activities were based on the use of both physical instruments and measures, and procedural controls of any irregularities and any aiding and abetting of criminal intentions. Physical instruments such as locks and keys and secured database and computer resources are used to inhibit unauthorised access and use of the resources for unauthorised operations. Procedural controls, such as protocols, filling of forms, verification of documents and required signatures, are also used to stop any fraudulent attempts. The standard activities used by most of the participants and suggested activities to improve prevention of online fraud included:

1. Physical security of computer resources and premises
2. Software security of data files – firewalls, anti-virus
3. Authentication of identity password, PIN, security codes
4. Authorisation of activities
5. Process check, control and verification

6.9.1.6 Detection Activities

Detection activities were based on the use of technological devices and internal system controls to discover intrusion, irregularities and security breaches. Security cameras and CCTV were to be installed to monitor customers in and around bank premises and ATMs. Automatic audit log of activities were also to be recorded for audit checks periodically. Daily transaction reports of account balances and movements were also to be made. Unusual and suspicious transactions were also to be flagged and instantly reported. Detection activities were therefore both real time and periodical. The activities therefore included:

1. Installation of security monitoring devices
2. Audit log
3. Periodic transaction reports
4. Automatic flagging of suspicious transactions

6.9.1.7 Remedy Activities

Remedy activities were based on the use of internal sanctions and the external legal system to seek redress and the punishment of offenders. Remedy activities are also aimed at using punitive measures to bring about correction of attitudes and behaviour, while serving as a warning to others who have the same intention to commit online fraud. Remedy activities therefore involved:

1. Procedures for enforcing sanctions.
2. Establishing appropriate punishment for different offences.
3. Establishing disciplinary procedures.
4. Global policy in relation to overseas fraud.

6.10 Summary

The study identifies issues of awareness/perception, regulations and enforcement and how they affected the effectiveness of the countermeasures adopted by the organisations. It also identified other external and internal environmental issues affected the countermeasures. The study highlights three major environments that have significant influence on countermeasure activities. The socio-cultural and religious environment of Saudi Arabia has a big influence on the people, organisation, and their practices; this influence may be positively used to combat online fraud. The financial/industrial

environment also had influence on the organisation putting pressure to modernise the banking sector which saw most banks adopting banking systems without much training and preparation. The study also confirms that organisational practices are more of direct responses to the demands of the socio-cultural and industrial sector environments than changes in technological advancements

CHAPTER 7

7. CONCLUSION

7.1 Introduction

The findings identified and discussed in previous chapters such as the impact of perception, awareness and other external and internal environmental influences on the effectiveness of countermeasures will form the bases of the study conclusion and consequently the recommendation and contributions of this research, in this chapter. The influence of the three major environments (socio-cultural; financial/industrial; and organisational environments) affecting the effectiveness of the countermeasures will be discussed to show how these influences may be positively used. A summary of the research which gives the flow of research activities will also be given in this chapter. Finally, the recommendations and the different contributions the study is making will also be discussed.

7.1 Research Summary / Major Findings

Chapter one introduced the problem background and observed the increasing rate of online fraud, in spite of the countermeasures put in place by the organisations and government of Saudi Arabia to control online fraud. It has increasingly become a problem and a major challenge to organisations and governments globally and specifically in the Gulf region (GCC). Combatting, controlling and preventing online fraud has therefore become a major focus of

most forward-looking organisations and governments in encouraging ecommerce and online transactions. This formed the basis and motivation for the research, resulting in the formulation of the research question, which seeks to determine how countermeasures by organisations in Saudi Arabia have affected the rate of online fraud.

The literature review in Chapter two identified the nature and type of online fraud in Saudi Arabia and reviewed the countermeasures put in place by organisations. This review indicated some problems and difficulties in combatting online fraud and the challenges of the countermeasures facing organisations. It identified the lack of legislation, inexperienced staff and the absence of comprehensive measures to fight online fraud, coupled with a lack of strategy and tactical awareness. It also suggested certain organisational, environmental and cultural issues that may affect the impact of the countermeasures adopted.

The discoveries of the issues raised in Chapter three, coupled with the aim of examining the impact of organisational activities and countermeasures on the deterrence, prevention, detection and remedy of online fraud in Saudi Arabia, helped in the choice of a theoretical base. The General Deterrence Theory (GDT) was chosen as a suitable theory, because of its argument for a systematic approach in the organisation and adoption of countermeasures to control online fraud. The theory identified four main components of countermeasures, which need to be systematically coordinated in order to create a positive and successful impact. The components, namely deterrence,

prevention, detection and remedy, therefore formed part of the theoretical framework that underpinned for the empirical investigation in the research.

The choice of the methodological approach was determined in Chapter four, based on the nature of the research, as identified in the literature review and the formulated theoretical framework. A qualitative method approach was chosen to ensure a broader and in-depth examination of the experiences of the participants from their own perspective, in their social and cultural context, that would enhance a balanced coverage of the subject matter as thematic analysis carried out on the qualitative data.

The findings of the analysis were presented in Chapters five (qualitative data, respectively). The qualitative analysis presented a deeper insight into the perceptions, technological measures, regulations and enforcement activities of persons and banking organisations that influenced online fraud activities. Chapter 6 presented the discussion and the interpretation of the findings. It identified the various countermeasures used in the organisations and highlighted the organisational, socio-cultural and environmental influences on the impact of the countermeasures. These findings, interpretations and discussions thus served as the bases for the recommendations.

7.2 Conclusions and Recommendations

The findings concluded that the expansion of ecommerce and online activities are being encouraged by the Saudi government with the active support of the banks, by the introduction of information technology facilities for banking services. However, this expansion of online activities and use of information

technologies in banking transactions also created opportunities and loopholes exploited by some online fraudsters, resulting in the loss of more than 20 million US dollars in 2010 and 2012 more the SR 2.6 billion (more than £100 Million) in 2012 (Arabnews,2012). The research identified a rise in online fraud, due to the large concentration of banks, increasing user base, the large number of financial transactions, poor security awareness and the perceptions of those involved (the socio-cultural environment and much more). This is in spite of the counter measures put in place by the government and the banks operating in the country.

As regards the research objective (to examine the countermeasures of deterrence, prevention, detection and remedy of online fraud used by organisations), it was concluded that, although most banks have introduced countermeasures, they mostly focus on prevention and detection. However, the findings suggest that the success of any effort or approach to combat fraudulent activities depends on the activities of the four countermeasure components. The activities of each component and the interrelationships of the components have a collective impact on combatting online fraud. The findings also conclude that the countermeasures adopted by most organisations are world standard, but too technical, complex in the Saudi context. Most subjects found the countermeasures difficult to use, mainly due to their socio-cultural background. This shows and confirms the importance and impact of the socio-cultural environment on the effectiveness of the countermeasures.

As regards the research objective to examine the impact of the countermeasures on online fraud, the findings conclude that the countermeasures are not comprehensive or sufficiently adequate to have affected the rate of online fraud, which remains high. There was no systematic approach adopted by the banks and government to the organisation and coordination of the components of the countermeasures, which the study confirms are interrelated. Further the findings also conclude that the lack of training, awareness and regulatory backings may have hindered the impact of the countermeasures. In addition, the findings conclude that the mind-set of the people, their perception and awareness of online fraud may have negatively influenced the impact of the countermeasures.

Finally the findings conclude that the socio-cultural, industrial and organisational environment have a significant effect on the impact of the countermeasures adopted by banks and the government. The influence of these environments on the countermeasures needs to be addressed to facilitate positive results (Figures 6 & 7).

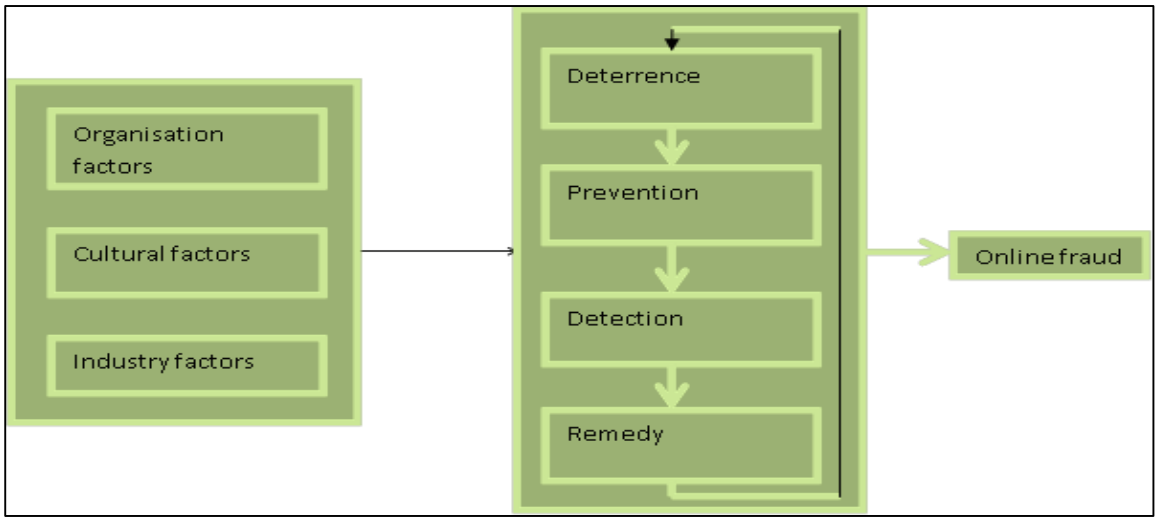


Figure 6 Factors effect on countermeasures

The findings (Figure 7) suggest that the socio-cultural, industrial and organisational environments may have individual and collective influence on the countermeasures. The direct influence of each environment and their collective influence must be identified and addressed to enhance the effectiveness of the countermeasures. The different environment may also have different impact on the different stages or phases of the countermeasures. For example, the socio-cultural environment may have different impact on deterrence that the organisational environment may have on deterrence. The impact of socio-cultural environment on prevention measures may also be different from its impact on detection countermeasures. Achieving effective countermeasures therefore require the identification of these different influences on the countermeasures and providing strategies or practices to eliminate or reduce to the minimum the influences.

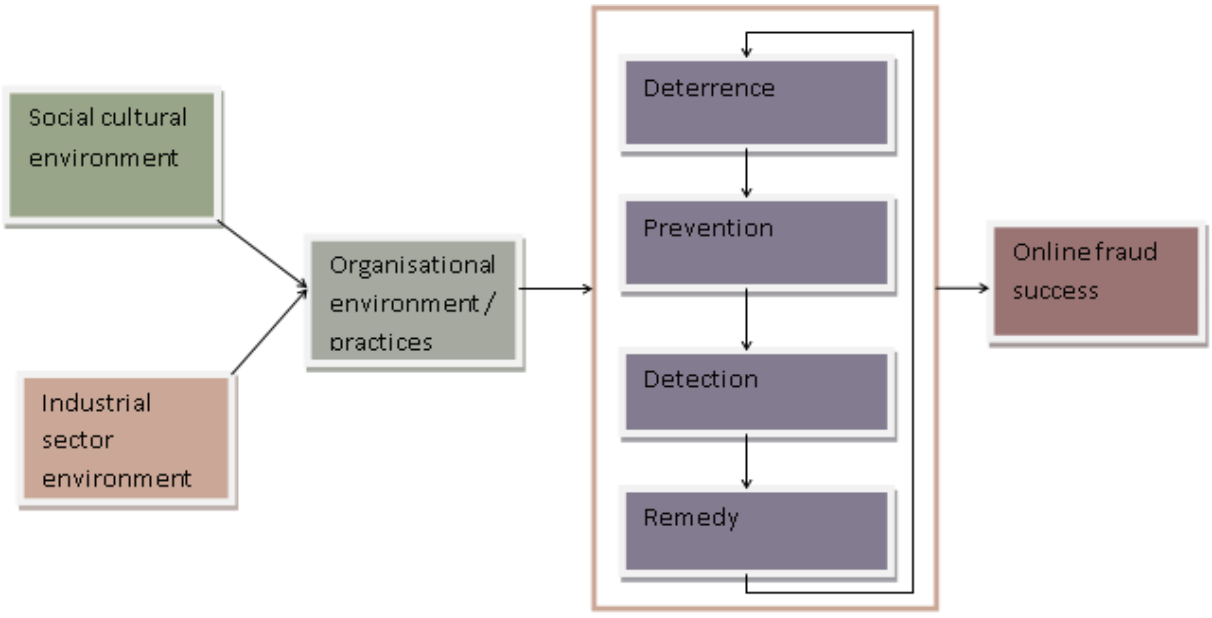
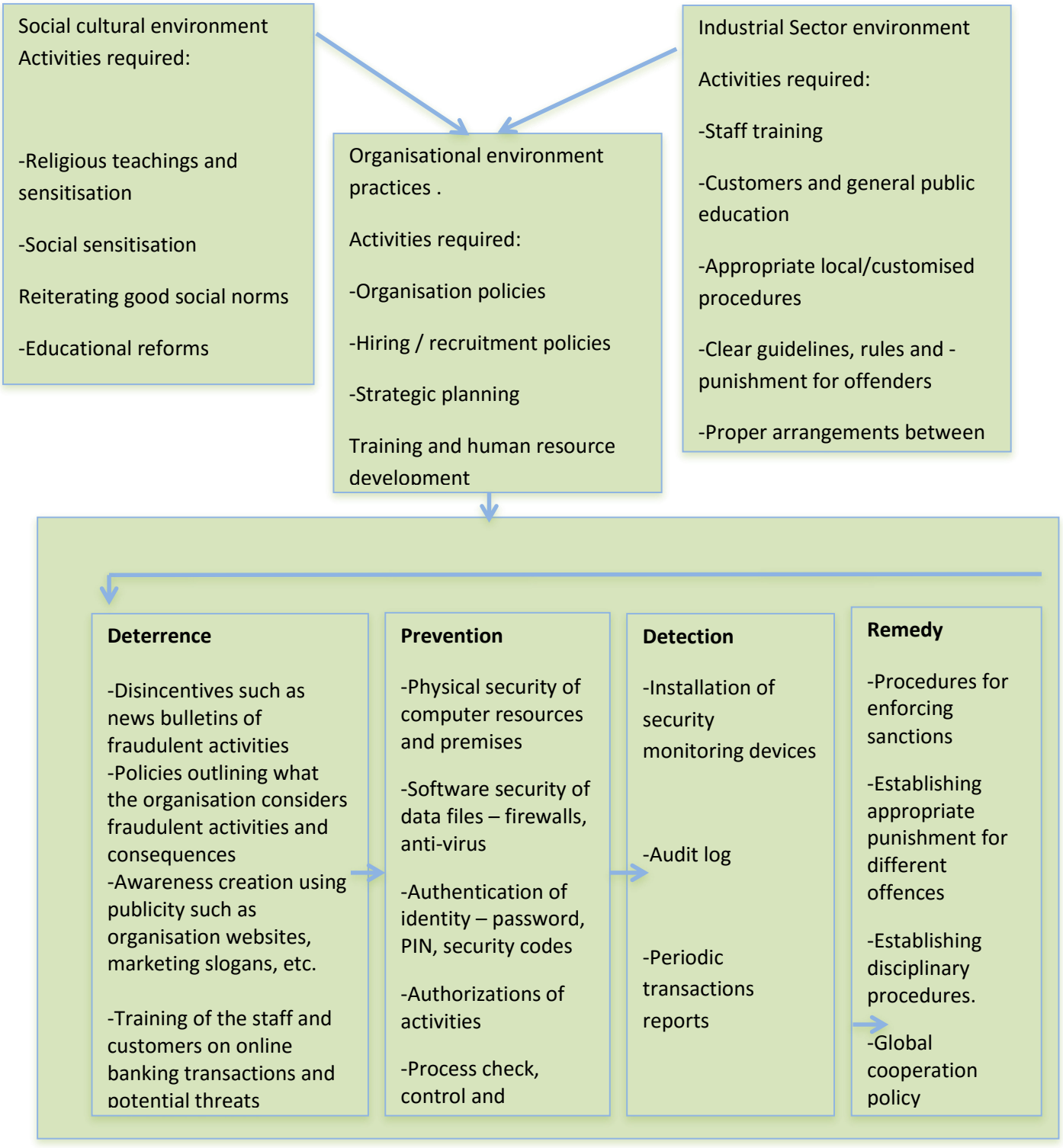


Figure 7 Impact on the countermeasures

The findings also suggest that the socio-cultural environment and the industrial environment of the banks directly influence organisational environment and impact on organisational practices of banks and financial institutions.



(Figure 8)Proposed model/Framework

The practices in most banks relating to the combat of online fraud therefore depend on best practices in the industrial environment and societal practices. These industrial and societal practices may have negative impact on the countermeasures, which needs to be identified. This suggests that the influence of the external environment of banks and financial institutions needs to be taken into consideration in formulating strategies to achieving effective countermeasures.

The recognition of the impact of the industrial and socio-cultural environments on organisational practices therefore suggests that positive activities and practices in these external environments may impact positively on the countermeasure activities of the banks and financial institutions. The influence of these environments may therefore be used positively to formulate positive strategies and countermeasures to effectively combat online fraud (Figure 8). The proposed model / framework therefore is based on the concept of identifying how the external environment with influences on organisational practices (which include countermeasures), can be used by introducing relevant activities in the environments to enhance the effectiveness of countermeasures.

7.3 Contributions

The study proposes a model that can be used as a practical solution to the issues of combatting fraud and using countermeasures effectively (see figure 8). The model is designed to address the issues identified in the study as major

challenges in creating a positive impact, with the countermeasures adopted by banks and the government in reducing the rate of online fraud in Saudi Arabia. The issues identified are as follows:

The meaning of online fraud and perceptions of it are based on cultural and societal beliefs and educational background and as such are difficult issue to tackle. Although online fraud is described as a deceptive act, it is also seen as a normal business affair carried out at a technological level. The mind-sets of the people are based on their moral, social, cultural and religious inclinations, which have formed different opinions and perceptions of online fraud. These opinions and perceptions need to be redirected in a positive direction .

The issues surrounding the levels of awareness and the challenges these issues pose for online occurrences in the country are important. The level of awareness is generally low, due to a lack of knowledge (including among bank staff and the public), training, and lack of government sensitisation and the religious inclinations of the population. The lack of a confidential reporting structure has also discouraged most victims from reporting their ordeals. The important Issues here are: types of technological and procedural controls, how these controls are designed, their main targets or focus and their relevance or adequacy. The measures adopted by the banks and government have varied purposes. While the majority focus on protecting computer resources, only a few are focused on protecting online activities. Some measures were described as irrelevant and cumbersome by a large proportion of customers and staff.

Regulations in the country and the impact on the prevention and combatting of online fraud are major challenges. The main issues and challenges are the effectiveness of the regulations and types of regulation, the focus on the regulations and their impact. There are government and organisational rules, with different foci and purposes, such as the monitoring of Internet operations and the provision of operational guidelines, which are regarded as very important. The enforcement of existing rules and regulations and bringing erring individuals and organisations to justice were minimal, owing to the passive and nonchalant attitude of the agencies. Although there were some legal and technological limitations and hindrances, the lack of knowledge and the unpreparedness of the staff and government constituted a major handicap and impediment to the prevention of online fraud in the country. The model proposes three-pronged coordinated environmental activities to address the identified issues. The model acknowledges the influence of these environments (socio-cultural, industrial and organisational environments) on these issues and therefore efforts to address them should derive from their use in the environment.

7.3.1 The Socio-cultural Environment's Impact on Countermeasures

The socio-cultural environment influences perceptions, awareness, social norms and the attitudes of the people. The prevailing social environment could therefore be a platform to address most of the issues, mitigating the effectiveness of the countermeasures. The activities proposed in the framework to be carried out are the following: see section 5.1.1.2 and section 5.1.13

Activities	Purpose	Examples
Religious teachings and sensitisation	To change the perception of the people about online fraud	- The evil of online fraud - Technological influence on the mind and religion
Social sensitisation	To create awareness and attitude of the people	- Creating awareness of the criminal nature of online fraud - Helping victims of online fraud through counselling
Reiteration of good social norms	To create positive social norms	- In the mosques - In other religious gatherings
Educational reforms in schools	To influence perception, awareness and attitude of the people	- Creating awareness of cybercrimes - Technological innovations and effects on society - Integration ICT in education

Table 11 socio-cultural environment activities

1. Religious teachings and sensitisation on

- The evil of online fraud
- Technological influence on the mind and religion
- Social sensitisation among social clubs and family unions
- Creating awareness of the criminal nature of online fraud
- Helping victims of online fraud through counselling

2.Reiteration of good social norms

- In the mosques
- In other religious gatherings

3. Educational reforms in schools
    - Creating awareness on cybercrimes
    - Technological innovations and effects on society
    - Integration ICT in education, schools.

Some of these activities are to some extent presently undertaken by most religious institutions, but there is a need to reiterate their importance in the fight against online fraud and to intensify their applications in every part of the country. Religious institutions need to do more, while educational institutions, social or business clubs and government bodies need to incorporate the teachings and sensitisations into their curricula. The model therefore proposes the use of the social environment through these activities to create a better attitude, based upon the better perceptions and awareness of online fraud and its dangers to individuals and the community. This attitude would help in the deterrence and prevention of online fraud.

7.3.2 Organisational Environment's Impact on Countermeasures

The organisational environment influences customers and staff awareness in terms of the training given to new and existing staff, publicity and the induction or orientation given to new customers. The organisational environment also influences the type, focus and implementation pattern of the procedural controls and technological measures adopted in the organisation, which have been highlighted as issues that affect the impact of the countermeasures. The enforcement of these controls and the effective running of the technological

measures have also been attributed to the organisational environment in terms of the knowledge and ability of the staff and sometimes the compromises and possible connivance of the staff with outsiders. The model therefore proposes the use of the organisational environment through the activities recommended to create customer and staff awareness and a good environment for the countermeasures. The activities proposed are: see section 5.2.1.1 and 5.2.1.2

1. Organisation policies on
    - Customers services/relationships
    - Bank's electronic banking and electronic commerce guidelines and help facilities available
    - Staff responsibilities
2. Hiring / recruitment policies
    - Importance and checking of references before employment
    - Staff induction and orientation
3. Strategic planning
4. Training and human resource development
5. Policy implementation

Activities	Purpose	Examples
Organisation policies	To create staff awareness and positive environment	- Customers services/relationships - E-banking and E-commerce guidelines - Staff responsibilities
Hiring / recruitment policies	To check the background credentials of staff and prevent the engagement of fraudulent staff	- checking of references before employment - Staff induction and orientation
Strategic planning	To create responsive staff and environment	- Regular updates of banking systems and procedures
Training and human resource development	To acquire up-to-date knowledge on countermeasures and online prevention	- Continuous professional development trainings
Policy implementation	To create organisational culture and awareness	- Enforcement of policies and rules

Table 12 Organisation environment activities

7.3.3 Industrial Environment's Impact on Countermeasures

Studies show that the financial service industry is very prone to attack, and thus requires staff to be more vigilant, professional and more aware to the ever changing fraudulent techniques that are consistently being invented by fraudsters. It also shows that standards and rules need to be set to guide

operators in the industry. They must be put in place and enforced. Careful assessments of those applying for sensitive positions within the industry must be carefully scrutinised for protection.

Employing only reputable and known people with verifiable and credible references also needs to be looked at. Thus the activities required are: see section 5.3.1.4 and 5.3.2.2

1. Staff training on
    - Cybercrimes, types, medium/platform/technologies used, prevention and detection.
    - Organisational policies and procedures.
    - Knowing your customers.

2. Customers and general public education.
    - Data protection
    - Password creation and regular updates
    - Organisational and banking rules, regulations and procedures
3. Appropriate local/customised procedures.
4. Clear guidelines, rules and -punishment for offenders.
5. Proper arrangements between Banks and Law enforcements.

Activities	Purpose	Examples
Staff training	To create an industry awareness and make staff more vigilant	- Cybercrimes types, platform and technologies used - Organisational policies and procedures - Knowing your customers
Customers and general public education	To educate the general public	- Data protection - Password creation and regular updates - Organisational and banking rules
Appropriate local/customised procedures	To set industry standards for operators	- Saudi banking sector procedures
Clear guidelines, rules and punishment for offenders	To clearly set online fraud laws	- Establishing Saudi government rules
Proper arrangements between Banks and Law enforcements	To ensure cooperation between banks and government agencies	- Establishing online fraud centre - Establishing reporting structure and working relationships between banks and the police

Table 13 Industrial environment activities

7.3.4 Validation of the Framework

Five industry experts on computer security and E-commerce provided positive feedback on the recommended framework, and agreed with the suggestion of exploring the influence of the environment positively to enhance the impact of the countermeasures. The importance of sensitizing the public and providing adequate training to staff were also emphasized.

"Education and training and raising awareness at all levels is the key to success in mitigating fraud" – (A consultant for an online payment service firm in Europe)

The framework is described as being capable of taking care of social, organisational and technical issues underlying online fraud in the country.

"In my years of experience as a Risk manager, I have never seen a model/framework that is this comprehensive and suitable for such a country " – (General Manager – Risk management of a Card company)

"The framework is very good as it considers the Saudi socio-cultural environment and organisation environment to fight online fraud rather than just using technological means" (Bank Manager)

These subjects also confirmed the adequate provision of the framework to handle what they called the "insider phenomenon", which has been a major issue in crime perpetration in banks. This is an issue where bank staff give out

sensitive data and information to their friends with criminal intention to defraud their organisations. Furthermore, the framework adopts both criminal-centred approaches and crime-centred approaches to provide balanced technical, formal, informal and social controls (Dhillon *et al*., 2004). It therefore emphasizes maximising opportunities to constrain potential offenders' behaviour, through the combined influences of the social, organisational, industry environments.

7.5 Theoretical Contributions

The General Deterrence Theory (GDT) provided a theoretical framework to investigate the countermeasures of deterrence, detection, prevention and remedy of online fraud in Saudi Arabia. It also helped in the critical analysis of these countermeasure activities, their interdependencies, interrelationships and impact on online fraud. The use of the theory identified the countermeasures adopted by the banks in Saudi Arabia and showed their interdependencies and impacts on online fraud. General Deterrence Theory (GDT) therefore focuses on countermeasure activities, relationships and their collective effect on online fraud. Its four components are based on the argument that individuals who commit crimes can be dissuaded from doing so with countermeasures (Straub and Welke, 1998). The countermeasures are therefore focused on altering the behaviours of the individual by influencing the decision-making of that individual, which may require altering or reinforcing how decision-makers perceive the key factors that need to be considered before they act.

The findings, however, show the influence of the environment on the effectiveness and impact of the countermeasure activities on online fraud, for which GDT does not make provision. The findings conclude and suggest the overriding importance of the three environments (socio-cultural, industrial and organisational). They conclude that the ineffectiveness of the countermeasures is based on environmental factors, and therefore suggest the importance of using the environment as a platform to create effective and better impacts on these environmental and behavioural issues.

Making the countermeasures work therefore depends very much on the environmental factors, and how such factors could be used to influence behaviours. Other computer security theories, such as criminological theory, information systems security effectiveness theory and situational crime prevention theory, also focus on environmental and physical security. This supports the inclusion of the environment in the working of GDT. A neglect of the influence of the environment is obvious in the theory, which must be taken into account.

GDT focuses on the behaviour of criminals (how they perceive fraudulent practices and factors) and therefore concentrates on altering decision-making behaviour and inhibiting criminal behaviour. The countermeasures must therefore be designed to affect behaviour and intentions. The findings, however, suggest that the behaviour of the population in Saudi Arabia is affected, largely directly and indirectly, by the identified environmental

influences, which need to be taken into account in the design and application of countermeasures to combat online fraud in Saudi Arabia.

The study therefore recommends that the influence of the environment should be seen as a factor and/or a major component of countermeasures to combat online fraud. It should therefore be incorporated into the theory to make it more comprehensive, covering every relevant area. The recommended framework suggests the inclusion of the environment in the systematic combatting of online fraud. Although GDT identifies the important components of countermeasures, the activities required to make an effective impact on online fraud and how best to systematically arrange the activities to gain a better collective impact have not been highlighted by the theory.

The present study highlights the importance of each component (their interdependencies and interrelationships) and therefore recommends a strong connection between the countermeasure activities and a systematic arrangement of the activities as suggested in the recommended framework (see figure 8).

The focus, application and implementation of the countermeasures have also proved to be key factors in the success of the theory. The research shows that the focus of some of the countermeasures was wrongly directed and ill-timed, and, as such, created negative impact. The application and the implementation processes also caused some customers discomfort and some embarrassment. The theory therefore needs to recognise the importance of these factors and

how they can be used to enhance the impact of the countermeasures. It also shows the need to adapt the theory to balance its perspectives and adopt balanced approaches, focusing on both the crime and the criminals (Beebe and Rao, 2005). Therefore, this model can help stakeholders such as law enforcements bodies, financial institutions and end users by creating the necessary environment and countermeasures to combat online fraud and such crime.

7.6 Critical Reflection

The sensitivity of the subject of study, the varied perceptions of its participants and the socio-cultural environment of in Saudi Arabia, made an interesting and challenging study , and affected the research in many ways, particularly in the design of the case study, the collection of the data and the interpretation of the results. The sensitivity of the subject matter (online fraud) attracted much interest from everyone connected with the study, both in the case study organisations and among members of the public, but only few of them agreed to share openly their experiences or be part of the study.

Most organisations at the start of the research initially agreed to participate in the research, but later on withdraw, because of the sensitivity and nature of the research. Some organisations agreed to participate on the condition that only general questions about the challenges of online fraud would be discussed, and not the specific online fraud they had encountered nor the countermeasures operating in their organisations. This general feeling of apprehension by the study population influenced the re-design of the study

focus and the methodological approach adopted for the research. It enhanced a rethink of the study aim and objectives and produced a more focused and clear workable study. The sensitive aspects of the subject were carefully omitted or made clearer for the participants to understand the motives behind the study.

The sensitivity of the subject matter, coupled with the stage of infancy of online fraud, was also responsible for the scarcity of data, reports and the literature. Only a few banks and organisations published their online fraud challenges. This also affected the research design and the methodological approach. A schedule of meetings was arranged with key officials from banks and organisations to have a better understanding of the situation. Social contacts and network of friends in the financial industry was put to good use to meet and convince staff of different organisations to be involved in the research. The social network thus provided a platform of trust and workable cooperation with relevant participants, even though some organisations remained impregnable. Nevertheless, a large proportion of the target organisations positively and effectively participated in the study. A decision was then taken to carry out a survey to have wider participation to obtain further responses and experiences. This facilitated the qualitative methodological approach adopted in the research. The varied perceptions and awareness of the participants about online fraud also brought some challenges in the data collection stage. The view that online fraud is a forbidden subject discouraged many participants. Those with online fraud victimization experiences, who viewed online fraud as a stigma - considering their social status - also initially refused to participate until

they were convinced of the confidentiality of the research. The socio-cultural environment of the country of focus also challenged the study in many ways.

7.7 Future Research

This research focused on the impact of the countermeasures adopted by the banks and the government on the rate of online fraud. This was done to determine the effectiveness of the countermeasures and the factors that had an impact on the effectiveness of the countermeasures. The findings however identified some environmental issues, including technological, social and organisational, which influenced the impact of the countermeasures. The findings also identified the rise in online fraud in certain activities in some cities and particular banks. A further study on these environmental issues and how / why they moderate the impact of the countermeasures on online fraud is thus recommended. More so, further studies may be on how the framework could be applied in other areas such as the public sector. In addition, further research can be carried out to identify the causes of online fraud in a similar religious or cultural environment and how such environment may influence the causes of online fraud.

7.8 Research Limitations

The study focused on the examination of measures and techniques adopted by Saudi financial organisations and how these have effectively controlled or prevented the issues of online fraud in the country. The study is therefore limited to the countermeasures designed and deployed by banks in Saudi Arabia to fight online fraud. The technical and economic feasibility of the

countermeasures were not the focus of this study and therefore were not fully examined. The study is also limited to specific online fraud related to online banking and e-commerce transactions. Other types of online fraud such as online auction fraud and other cybercrimes were not examined in the domain of the study. The study was also limited to the effect of the environment on the countermeasures and not on the evolvement of the environment and forces in the environment.

BIBLIOGRAPHY

AAG (Arab Advisor Group) (2011), *Saudi Arabia's Internet users spent around US$ 3 billion in 2010 on buying products and services through e-commerce*, Arab Advisor Group, available at: <http://www.arabadvisors.com/Pressers/presser-170211.htm>. (Accessed: February 2015)

Abdalla, S. & Albadri, F. (2010). *ICT Acceptance, Investment and Organization: Cultural Practices, and Values in the Arab World*. New York, NY: IGI Global.

ACG (Alpen Capital Group) (2009), *GCC Retail Industry*, Alpen Capital Group.

Ackroyd, S. & Fleetwood, S. (Eds.). (2000). Realist perspectives on management and organisations. *Psychology Press*.

Adams, R. (2010). Prevent, protect, pursue preventing fraud*. Computer Fraud & Security,* 2010, (7) pp 5-11 available at : http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=52878189 (Accessed: 6 January 2015).

Adler, P. S. and Kwon, S. W (2002). "Social Capital: Prospects for a New Concept," *Academy of Management Review* (27:1), pp. 17-40.

Ahmed, S., Buragga, K. & Ramani, A. K. (2011, February). Security issues concern for E-Learning by Saudi universities. In Advanced Communication Technology (ICACT), 2011 13th International Conference on (pp. 1579-1582). *IEEE*.

Al Somali, Z. & Ghinea, G. (2012). Investigation of factors affecting growth of e-banking services in Saudi Arabia. In Internet Technology and Secured Transactions, 2012 International Conference (pp. 583-588). *IEEE*.

Al-Otaibi, M. B. & Al-Zahrani, R. M. 2003. E-commerce adoption in Saudi Arabia: An evaluation of commercial Organizations' web sites. In *Proceedings of the International Conference on Information Technology in Asia* (CITA) pp. 26-31.

Alarabiya (2013) hackers-sabotage-government-websites available at http://english.alarabiya.net/en/media/2013/05/18/Saudi-Arabia-says-.html. (Accessed: 13 February ,2015).

Alasuutari P. (1995), *Researching Culture: Qualitative Method and Cultural Studies,* London, UK. Sage Publications.

Alavi, M. and Carlson, P. (1992), A review of MIS research and disciplinary development, *Journal of Management Information Systems* (8:4), pp. 45-62.

Albert, M. R. (2002). E-buyer beware: why online auction fraud should be regulated. *American Business Law Journal*, 39(4), 575-644.

Albrecht, W., Albrecht, C., Albrecht, C. & Zimbelman, M. (2011). *Fraud examination. South Western OH*, *USA*, Cengage Learning.

Alfuraih, S. (2008), *E-commerce and E-commerce Fraud in Saudi Arabia: A Case Study'*, in 2nd International Conference on Information Security and Assurance Busan, Korea, pp. 176-80

AlGhamdi, R., Drew, S. & AlFaraj, O. (2011). Issues influencing Saudi customers' decisions to purchase from online retailers in the KSA: A qualitative analysis. *European Journal of Scientific Research*, *55*(4), 580-593.

Alicia B. (2012) *Biggest Banks In Saudi Arabia,* available at: http://gulfbusiness.com/2012/08/top-banks-in-saudi-arabia/#.UoosBWNQWEA (Accessed 12 February 2015).

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, *3*(3), 176-183.

Al-Tawil, K., Sait, S. & Hussain, S. (2003). Use and Effect of Internet in Saudi Arabia', In *The 6th World Multi-Conference on Systemic*.

Anderson, E. (2000). *Code of the street: Decency, violence and the moral life of the inner city*. WW Norton & Company

Angelakopoulos, G. & Mihiotis, A. (2011). E-banking: challenges and opportunities in the Greek banking sector*. Electronic Commerce Research,* 11(3), pp. 297–319.

Antony S, Lin Z & Xu B (2006). Determinants of escrow service adoption in consumer-to-consumer online auction market: an experimental study, Decision. *Support Systems*. 42(3):1889-1900

Arabnews (2012) *Cybercrime costs Saudi Arabia SR 2.6 bn a year*, available at http://www.arabnews.com/saudi-arabia/cybercrime-costs-saudi-arabia-sr-26-bn-year (accessed: 12 February, 2015).

Aransiola, J. O. & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), pp. 759-763.

Archer S., (1988), Qualitative research and the epistemological problems of the management disciplines. In *Competitiveness and the Management Process* Basil Blackwell, Oxford (Pettigrew A, Ed.), pp. 265-302.

Arnold C.E. (2008), *How You Can Profit from Credit Cards: Using Credit to Improve Your Financial Life and Bottom Line*, FT Press; 1st edition

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research*. Qualitative Research, 1(3), pp. 385-405*.

Auta, E. M. (2010). E-banking in developing economy*:* Empirical evidence from Nigeria*. Journal of Applied Quantitative Methods*, Vol.5 (2):212-222.

Avison, D. E. & Pries-Heje, J. (Eds) (2005). *Research in information systems: A handbook for research supervisors and their students*. Gulf Professional Publishing.

Baden M.S. and Wilkie K. (2004), *Challenging Research in Problem Based Learning*, Open University Press.

Bajari, P. & Hortacsu, A. (2003). Economic insights from internet auctions: A survey (No. w10076). *National Bureau of Economic Research*.

Bartling, S. & Friesike, S. (Eds) (2014). *Opening Science*. Cham: Springer International Publishing.

Becker, H. (1963) *Outsiders*: *Studies in the Sociology of Deviance.* New York: Free Press.

Beebe, N. L. and Rao, V. S. (2005), Using Situational Crime Prevention Theory to explain the effectiveness of information systems security, In *Proceedings of the 2005 Software Conference*, Las Vegas, NV, pp 1-18.

Bennett, S. F. (1995) Community Organizations and Crime*,* in *Annals of the American Academy of Political and Social Science*, Sage Publications, Newbury Park, CA, pp. 72-84.

Benjamin, O. A. & Samson, B. S. (2011). Effect of perceived inequality and perceived job insecurity on fraudulent intent of bank employees in Nigeria. *Europe's Journal of Psychology, 7(1),* pp 99-111.

Benton T. and Craib I. (2001), *Philosophy of Social Science: The Philosophical Foundations of Social Thought*, New York: Palgrave Macmillan.

Beresford, A. (2003) *Securities/Investment Fraud.* Washington, DC: National White Collar Crime Centre Bryman

Berg, B.L. (2001), *Qualitative Research Methods for Social Sciences*, 4th edition, USA. Allyn and Bacon.

Bhattacharyya, D., Ranjan, R., Alisherov, F. & Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*, 2(3), 13-28.

Biegelman, M.T. and Bartow, J.T. (2012), *Executive Roadmap to Fraud Prevention and Internal Control: Creating a Culture of Compliance other formats*, 2nd edition New Jersey, USA, John Wiley & Sons.

Black S. and Ferguson E. (2011), *Forensic Anthropology: 2000 to 2010*, FL. USA, Taylor & Francis

Blanco Hache, A. C. & Ryder, N. (2011). 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas: 1 a critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud. *Information & Communications Technology Law*, 20(1), 35-56.

Bourgois, P. (1996) *In Search of Respect Selling Crack in El Barrio*, Cambridge University Press, New York,

Boyatzis, R.E. (1998), *Transforming qualitative information: Thematic analysis and code development*, California, Sage publications Ltd.

Braun, V. & Clarke, V. (2006), "Using thematic analysis in psychology"*, Qualitative Research in Psychology*. (3) pp. 77-101.

Brenner S.W. (2010), *Cybercrime: Criminal Threats from Cyberspace*, California, Praeger.

Brenner S.W. (2012) *Cybercrime and the Law: Challenges, Issues, and Outcomes, Boston,* Northeastern University press.

Brewer, J. D., Lockhart, B. and Rodgers, P. (1998), "Informal Social Control and Crime Management in Belfast," *The British Journal of Sociology* (49:4), pp. 570-585.

Bridges D. & Smith R.D. (2007), Philosophy, Methodology and Educational Research, *Journal of Philosophy of Education*, Wiley-Blackwell: 1st edition.

Brodie, R. J., Winklhofer, H., Coviello, N. E. & Johnston, W. J. (2007). Is e-marketing coming of age? An examination of the penetration of e-marketing and firm performance*. Journal of Interactive Marketing*, 21(1), 2-21.

Bryant, R. (2008). *Investigating Digital Crime*. Chichester. England: Wiley.

Bryman, A. & Bell, E. (2003) *Business Research Methods*, Oxford University Press, Oxford.

Bryman, A. (2012). *Social research methods*. Oxford, Oxford University Press.

Burgess, R. L. and Akers, R. L. (1966), A Differential Association-Reinforcement Theory of Criminal Behavior, *Social Problems*, 14, 128-147.

Bursik, R. J. (1988), “Social Disorganization and Theories of Crime and Delinquency: Problems and Prospects,” *Criminology* (26:4), pp. 519-551.

Carifio, J. & Perla, R. (2007), *Ten Common Misunderstandings*, Misconceptions, Persistent Myths and Urban Legends about Likert Scales and Likert Response Formats and their Antidotes. *Journal of Social Sciences*, 2, 106-116.

Cendrowski, H., Petro, L. W., Martin, J. P. & Wadecki, A. A. (2007). *The handbook of fraud deterrence*. Hoboken, New Jersey John Wiley & Sons.

Cha, A. (2005), “*Police Find That on eBay Some Items Are a Real Steal*”, available: http://www.duluthsuperior.com/mld/duluthsuperior/10597328.html; accessed 17/08/06 (Accessed: January 2015).

Chantler, N. (1996). *Profile of a computer hacker*. Faculty of Law, Queensland Australia. University of Technology.

Choplin, J. M., Stark, D. P. & Ahmad, J. N. (2011). Psychological Investigation of Consumer Vulnerability to Fraud: Legal and Policy Implication, *A. Law & Psychol. Rev*., 35, 61.
Clarke, R. V. (1980) Situational Crime Prevention: Theory and Practice, *British Journal of Criminology*, 20, 136-147.

Clarke, R. V. (1997) *Situational Crime Prevention: Successful Case Studies*, Publishers: Guilderland, NY, Harrow and Heston.

Clifford R.D. (2011), *Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime*, Carolina Academic Press; 3 edition.

Coenen T. (2009), *Expert Fraud Investigation: A Step-by-Step* Guide, New Jersey, Wiley & Sons, 1st edition.

Cole, K. (2004) '*When eBay Bargains Are a Little Too Hot'*, available at: cbsnewyork.com/topstories/local_story_134071152.html (Accessed: 5 January 2015).

Collis, J. and Hussey, R. (2003), *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*, Palgrave Macmillan, Houndmills, Basingstoke, Hampshire.

Cornish, D. and Clarke, R. V. (1986). *The Reasoning Criminal*, Springer-Verlag, New York.

Costanzo L.A. and MacKay R.B. (2010), *Handbook of Research on Strategy and Foresight*, Edward Elgar Publishing Ltd; Reprint edition.

Creswell J.W. (2008), *Research Design: Qualitative, Quantitative and Mixed Methods Approaches,* USA, Sage Publications, Inc, Third Edition.

Creswell, J.W. (2007), *Qualitative inquiry and research design: Choosing among five traditions 2*nd edition,Thousand Oaks, CA., Sage.

Criteo (2015), *eCommerce Industry Outlook*, available at http://www.criteo.com/media/1432/criteo-ecommerce-industry-outlook-2015.pdf (Accessed: 13, April, 2015).

Cross, M. (2008), *Scene of cybercrime*. New York: Syngress Elsevier.

Cullen F.T. & Wilcox P. (2010), *Encyclopedia of Criminological Theory*, Online Pub. November 23, pp. 561-566 doi: 10.4135/9781412959193

Curry, S. (2005) '*Online Auctions: The Bizarre Bazaar'*, available at: http://www.scambusters.org/onlineauctions.pdf (accessed 9 December, 2014).

Daswani. N, Kern C. and Kesavan A. (2007), *Foundations of Security: What Every Programmer Needs to Know,* 1st edition, New York Press.

Davies M.B. (2007), *Doing a Successful Research Project: Using Qualitative or Quantitative Methods*, Palgrave Macmillan.

Dawson C. (2009), *Introduction to Research Methods: A Practical Guide for Anyone Undertaking a Research Project,* How To Books Ltd; 4th Revised edition.

Deloitte, (2011), *Facing the Challenge of Fraud. GCC* Fraud Survey. Available at: http://www.docstoc.com/docs/81168458/GCC-fraud--survey-2011-Facing-the--challenge-of-fraud-by-deloitte (Accessed: 12th January, 2015).

Denning, D. (1998) *Information Warfare & Security,* Boston, Addison-Wesley: Reading, pp. 1-522.

Dhillon, G., Silva, L. and Backhouse, J. (2004) Computer Crime at CEFORMA: A Case Study, *International Journal of Information Management*, 24, pp. 551-561.

Dodge, R. C., Carver, C. & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), pp. 73-80.

Dolan, K. M. & Agent, S. (2004). Internet auction fraud: the silent victims. *Journal of Economic Crime Management*, 2(1), pp.1-22.

Drake P. and Heath L. (2010), *Practitioner Research at Doctoral Level: Developing Coherent Research Methodologies*, New York, Routledge.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, 14(4), pp.532-550.

Elden, M. and Chisholm, R.F. (1993), Emerging Varieties of Action Research: Introduction to the Special Issue, *Human Relations* (46:2), pp. 121-14

El-Guindy M.N. (2008), Cybercrime in the Middle East, *SSA Journal,* Egypt, June.

Elnaim, Bushra Mohamed Elamin (2013). Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future. *Information and Knowledge Management. Vol. 3, No. 12.*

eMarketer. (2001),*'The ePrivacy and security report.'* White paper available at: by MarketResearch.com. (Accessed: 28 January 2014).

English, E. (1996) 'SEC Tackles Internet Investment Fraud', *Network Security*, January 1996: 8.

Enos, L. (2000) '*Yahoo! Sued for Auctioning Counterfeit Goods'*, available at: http://www.ecommercetimes.com/story/2849.html. (Accessed 13 January 2015).

Eriksson P. and Kovalainen A. (2008), *Qualitative Methods in Business Research*, London, Sage Publications Ltd

Falaki, S. O., Alese, B. K., Adewale, O. S., Ayeni, J. O., Aderounmu, G. A. & Ismaila, W. O. (2012). Probabilistic Credit Card Fraud Detection System in Online Transactions. *International Journal of Software Engineering & its Applications*, 6(4).

Falcone R., Singh M. and Tan Y.H. (2002), Trust in Cyber-societies*: Integrating the Human and Artificial Perspectives*, Berlin: Springer, pp. 27-54.

Fettweis, G. & Alamouti, S. (2014). TU Dresden. *Communications Magazine, IEEE*, *52*(2), pp.140-145.

Financial Fraud Action UK. (2009). 'Financial Fraud Action UK announces latest fraud figures', 7th October. Available at: http://www.banksafeonline.org.uk/documents/2009H1Fraud PressRelease.pdf (Accessed: 14 January 2015).

Financial Services Authority (2000), *E-banking: risks and responses*. 29th March, Available:http://www.fsa.gov.uk/Pages/Library/Communication/Speeches/2000/sp46.shtml (Accessed: January 2015)

Fisher J. (2004), E-mail authentication slams spam, *Computer Technology Review*. Available at: http://wwpi.com/e-mail-authentication-slams-spam-2/ (Accessed 18 January 2015).

Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace. *Journal of Financial Crime, 14 (2), pp.190–207.*

Flick U. (2011), *Introducing Research Methodology:* A Beginner's Guide to Doing a Research Project, London, Sage Publications Ltd.

Foucault, M (1977). *Discipline and Punish: The Birth of the Prison*, Penguin, London,

Fraud Advisory Panel. (2009). *Fraud facts: cybercrime – social networks and virtual world*, October. Available at: http://www.fraudadvisorypanel.org/newsite/pdf_show.php? (Accessed: 25, January 2015).

Fried, R. (2001), *'Cyber Scam Artists: A New Kind of .con',* available at: http://www.crime-sceneinvestigator.net/CyberScam.pdf (Accessed 20 January 2015).

Galliers, R. D. (1991), “Strategic information systems planning: myths, reality and guidelines for successful implementation” *European Journal of Information Systems*, 1(1), pp. 55-64.

Garlik. (2009). *UK cybercrime report 2009, September*. Available at: www.garlik.com/press. php?id¼613 9 (Accessed:14 August 2014).

Goffman, E. (1969), *The Presentation of Self in Everyday Life*. Harmondsworth: Penguin.

González, M.E., Dentiste, M.R. and Rhonda, M.W. (2008), An alternative approach in service quality: an e-banking case study, *The Quality Management Journal, Vol. 15, No. 1, p. 41.*

Goodrich M. & Tamassia R. (2010), *Introduction to Computer Security,* Addison Wesley; 1st edition.

Gordon, S. & Ford, R. (2002). Cyberterrorism? Computers & Security*, The International Library of Essays in Terrorism*, Alan O’Day 21 (7), pp. 636–647.

Gordon, S. & Ford, R. (2006). On the definition and classification of cybercrime*. Journal in Computer Virology, 2 (1), pp. 13–20.*

Gragido W. and Pirc J. (2011), Cybercrime and Espionage: *An Analysis of Subversive Multi-Vector Threats,* Syngress; 1st edition

Grazioli, S., Johnson, P. E. & Jamal, K. (2006). A cognitive approach to fraud detection. *Journal of Forensic Accounting*, 7(1), pp. 65-88.

Hafner, K. (2004), *With Internet fraud up sharply, eBay attracts vigilantes*, New York Times, 20, Mar, 20.

Haken H. (2010), *Synergetic Computers and Cognition: A Top-Down Approach to Neural Nets*, Berlin, Springer.

Harrison, G. W. & List, J. A. (2004). Field experiments, *Journal of Economic Literature, pp.1009-1055.*

Harrison, A., Mennecke, B. & Dilla, W. (2012). An Empirical Study of a Two-Sided Model of Fraudulent Exchange. *ICIS 2012 Proceedings, Orlando*.

Hassie-Bibber, S.N. & Leavy, P. (2006), *The Practice of Qualitative Research,* SAGE Publication, Cal.

Hawkins, S., Yen, D. C. & Chou, D. C. (2000). Awareness and challenges of Internet security. *Information Management & Computer Security*, *8*(3), pp.131-143.

Hayes, N. (Ed.) (1997). Theory-led thematic analysis: social identification in small companies*. Doing Qualitative Analysis in Psychology,* Psychology Press, Hove, UK.

Hennink M., Hutter, I. & Bailey, A. (2011), *Qualitative Research Methods*, SAGE Publications Ltd, London.

Higgins G. (2009), *Cybercrime: An Introduction to an Emerging Phenomenon*, McGraw-Hill Humanities/Social Sciences/Languages, 1st edition.

Hirschheim R., Klein H.K. and Lyytinen K. (1995), *Information Systems Development and Data Modeling: Conceptual and Philosophical Foundati*ons, Cambridge University Press.

Hirschheim, R. (1985). Information systems epistemology: An historical perspective. *Research methods in information systems*, pp.13-35.

Hirschi, T. (1969). *Causes of Delinquency*, University of California Press, Berkeley, CA,

Holt T. (2012), *Cybercrime and Criminological Theory*: *Fundamental Readings on Hacking, Piracy, Theft and Harassment*, Cognella Academic Publishing

Hollinger, R. D., & Clark, J. P. (1983). Theft by employees. Lexington, MA: Lexington Books

Hunton, P. (2009). The growing phenomenon of crime and the Internet: a cybercrime execution and analysis model. *Computer Law & Security Review*, 25, pp. 528–535

Internet Crime Complaint Center (2007) available at: https://www.ic3.gov/media/annualreports.aspx (Accessed: 23 January 2015).

International Monetary Fund (2012) Saudi Arabia: Reports on the Observance of Standards and Codes

Internet crime report (2013), available at: http://www.ic3.gov/media/annualreport/2013_IC3Report (Accessed 23 January 2015).

Jankowski N.W. and Jensen K. B. (2007), *A Handbook of Qualitative Methodologies for Mass Communication Research*, New York, Taylor & Francis Group, Routledge.

Jasimuddin, Sajjad M. (2001), Saudi Arabian banks on the web. *Journal of Internet Banking and Commerce* (6.) 1.

Jensen P.A. and Bard J.F. (2002), *Operations Research Models and Methods*, John Hoboken, NJ, Wiley & Sons.

Jewkes, Y. (2010) 'Public Policing and the Internet' in Y. Jewkes and M. Yar (eds.) *Handbook of Internet Crime*, Cullompton: Willan

Joint Research Centre (2011), *Experimental Results and Population Response for Selected Chemicals: Studied Site and Sampling Collections*, Dictus Publishing.

Jøsang, Audun et al. (2007), Security Usability Principles for Vulnerability Analysis and Risk Assessment, Proceedings of the Annual Computer Security Applications Conference, 2007. ACSAC 2007, Twenty-Third Annual*. IEEE.*

Kamaruzaman, Khairun Nisah, Yasmin Magdalena Handrich and F. Sullivan (2010). E-commerce adoption in Malaysia: Trends, issues and opportunities. *ICT strategic review.*

Kaplan, Ronald M., and John T. Maxwell III. (1994). *Text-compression technique using frequency-ordered array of word-number mappers*. U.S. Patent No. 5,325,091.

Kaspersky (2014) *Kaspersky security Bulletin*, Overall statistics available at: https://securelist.com/files/2014/12/Kaspersky-Security-Bulletin-2014. -Overall-statistics-for-2014.pdf (Accessed: 20th February 2015)

Katz J. (2010), *Digital Signatures,* 1st Edition, r; New York, Springe, 2nd Printing.

Kearney. (2013) Online Banking in the GCC available at: http://www.atkearney.com/web/digital-business-forum/detail/-/asset_publisher/VMEx2L1PhjPS/content/online-banking-in-the-gcc/10192 (Accessed: 13 January 2015)

Keddie N.R. (2006), *Women in the Middle East: Past and Present*, Princeton University Press, illustrated edition.

Khan, M. S. and Mahapatra, S. S. (2009). Service quality evaluation in Internet banking: an empirical study in India. *Int. J. Indian Culture and Business Management*, 2(1), pp. 30-46.

Khanna N., Mikkilineni A.K., Martone A.F. and Ali G. (2006), A survey of forensic characterization methods for physical devices, *Digital Investigation*, Elsevier.

Kirwan G. and Power A. (2013) *Cybercrime: The Psychology of Online Offenders,* Cambridge University Press.

Klein, H.K. & Myers, M.D. (1999), A set of principles for conducting and evaluating interpretive field studies in Information Systems", *MIS Quarterly: Management Information Systems, (*23), no. 1, pp. 67-94.

Kothar CR (2004), *Education Research Methodology: Methods and. Techniques,* New Delhi: New Age International.

Kotulic, A. G. & Clark, J. G. (2004). *Wh*y there aren't more information security research studies. *Information & Management, 41(5), pp. 597-607.*

Kou, Y., Lu, C. T., Sirwongwattana, S. & Huang, Y. P. (2004). Survey of fraud detection techniques. In Networking, sensing and control*, IEEE international conference (2,) pp. 749-754.*

Krone, T. (2005). *High tech crime brief* no. 1. Canberra: Australian Institute of Criminology. Available at: http://www.aic.gov.au/documents/6/B/6/%7B6B679000–637F–4A27– 9229–3C42928B364B%7Dhtcb001.pdf (Accessed: 25 February 2015).

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives.* Springer Science & Business Media.

Kshetri N. (2010), *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*, Springer-Verlag Berlin Heidelberg

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security and Privacy, 4(1), pp. 33–39.*

Kubrin, C. E. and Weitzer, R. (2003), New Directions in Social Disorganization Theory, *Journal of Research in Crime and Delinquency* (40:4), pp. 374-402

Kumar R. (2010), *Research Methodology: A Step-by-Step Guide for Beginners*, Third Edition. London. Sage Publications Ltd.

Kumaraguru P., S. Sheng, A. Acquisti, L. Cranor and J. Hong (2008), Lessons From a Real World Evaluation of Anti-Phishing Training, in *Proc of the IEEE eCrime Researchers Summit, pp. 1-12*

Kvale, Steinar (1996), Interviews*: An Introduction to Qualitative Research Interviewing*, Sage, London.

Lapadat, J. C. & Lindsay, A. C. (1999), Transcription in Research and Practice: From Standardization of Technique to Interpretive Positionings. *Qualitative Inquiry, 5(1), pp. 64-86.*

Laudon, K. C. & Traver, C. G. (2007). *E-commerce,* Pearson/Addison Wesley.

Leeson, P. T. & Coyne, C. J. (2005). Economics of Computer Hacking, *The JL Econ. & Pol'y*, *1*, 511.

Long J., Mullen T. and Russell R. (2007), *Stealing the Network: How to Own a Shadow,* MA, Syngress; 1 edition, Rockland.

Mann, Catherine L. (2000) Electronic Commerce in Developing Countries. *Washington DC: Institute for International Economics. Working Paper 3.*

Marcus, L. & Robey, D. (1998), "Information technology and organisational change: causal structure in theory and research", *Management Science*, vol. 34, no. 5, pp. 583-598.

Martin, W. E. & Bridgmon, K. D. (2012). *Quantitative and statistical research methods: from hypothesis to results,* Vol. 42., John Wiley & Sons, Jossy Bas, San Francisco.

Martin, E. (ed.) (2003) *Oxford Dictionary of Law, 5th edn*. Oxford University Press, Oxford.

Masocha, Reginald, Norman Chiliya and Stanislous Zindiye (2011) E-banking adoption by customers in the rural milieus of South Africa*:* A case of Alice, Eastern Cape, South Africa*."African Journal of Business Management",* 5.5, pp. 1857-1863*.*

Mayes K. and Markantonakis K. (2010), *Smart Cards, Tokens, Security and Applications,* Verlag Springer, Softcover reprint of hardcover, 1st ed.

Mayes E. & Lynas N. (2011), *Credit Scoring for Risk Managers*: *The Handbook for Lenders*, CreateSpace.

McIntyre A. (2007), *Participatory Action Research*, Sage Publications, Inc.

MCIT (2010) (Saudi Ministry of Communication and Information Technology), *ICT indicators in K.S.A* (Q3-010), available at: http://www.mcit.gov.sa/english/Development/SectorIndices/ (Accessed : 28 February 2015).

McJohn S.M. (2009), *Glannon Guide To Commercial Paper & Payment Systems*, Wolters Kluwer Law & Business, New York.

McNiff J. and Whitehead A.J. (2009), *Doing and Writing Action Research,* Sage Publications Ltd, London

McQuade III S.C. (2005), *Understanding and Managing Cybercrime*, Prentice Hall; 1 edition, New Jersey

McQuade, III. S. (2009), *Encyclopedia of cybercrime*, Greenwood Press, New York.

Metropolitan Police Service. (2008). *Sterling: an economic crime strategy for London – Report 2005–2008.* London: Metropolitan Police Service.

Microsoft (2012) Online Fraud: Your Guide to Prevention, Detection and Recovery, available at:http://download.microsoft.com/download/9/D/C/9DC0FC43-57F4-4723-8C39-3CB0FBB15E30/OnlineFraud_Booklet.pdf. (Accessed: 12 May 2015).

Mingers, J. (2001), Combining IS Research Methods: Towards a Pluralist Methodology, *Information Systems Research*, vol. 12, no. 3, pp. 240-259.

Miyazaki, A. D. & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, *19*(1), pp. 54-61.

Mokhtar, I., Osman, I., Setapa, F. & Zambahari, S. R. (2015, January). A Qualitative Study on the Determinants of Islamic Credit Card Ownership and Usage. In *Proceedings of the Colloquium on Administrative Science and Technology* (pp. 423-435). Springer Singapore.

Montague D. (2011), *Essentials of Online Payment Security and Fraud Prevention*, New York, John Wiley & Sons, Inc.,

Montealegre, R. (1999a), A Case for More Case Study Research in the Implementation of Information Technology in Less-Developed Countries*, Information Technology for Development,* vol. (8), no. 4, pp. 199-207.

Moore R. (2014), *Cybercrime: Investigating High-Technology Computer Crime,* Routledge; 2 edition, London

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A. & Elovici, Y. (2009). Identity theft, computers and behavioral biometrics. In Intelligence and Security Informatics, ISI'09*. IEEE International Conference* (pp. 155-160).

MPAA (Motion Picture Association of America) (2002) 'U*.S. Entertainment Industry: MPA Market Statistics'*, available: at http://www.mpaa.org (Accessed: 29 January 2015).

Mullarney J.X. (2005), *E-Commerce Creates Unique Exposures, National Underwriter Property & Casualty-Risk & Benefits Management*, The National Underwriter Company.

Murdoch, S. & Anderson, R. (2010), "Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication," In *Financial Cryptography and Data Security*, 6052 ed. R. Sion, Springer, Berlin Heidelberg.

Myers, M.D. (2009), *Qualitative research in business & management*, 1st ed, London. Sage publications Ltd,

Myers, M. D., (1997). Qualitative research in information systems*. Management Information Systems Quarterly*, Sage publication, *21*, pp 241-242. London.

Nance, W.D. and Straub, D.W. (1988), An Investigation into the Use and Usefulness of Security Software in Detecting Computer Abuse, "*Proceedings of the Ninth International Conference on Information Systems*, J.I. DeGloss and M. H. Olson (eds), Minneapolis, MN, pp. 283-294.

Napier H. A., Rivers O. N. and Wagner S. (2005), *Creating a Winning E-Business, Course Technology*; 2nd edition, Boston, Thomson.

Nash, J. (1976), *Hustlers and Con Men: An Anecdotal History of the Confidence Man and His Games,* New York: M. Evans.

National White Collar Crime Center and the Federal Bureau of Investigation (March, 2009). Available at: https://www.fbi.gov/news/pressrel/press-releases/fbi-national-white-collar-crime-center-nw3c-release (Accessed: 12 April 2015).

Nichols R.K. and Lekkas P.C. (2001), *Wireless Security: Models, Threats, and Solutions,* 1st edition. US. McGraw-Hill Professional.

Nolan III, J. J., Conti, N. and McDevitt, J. (2004) “Situational Policing: Neighborhood Development and Crime Control,” *Policing & Society* (14:2), pp. 99-117.

O'Hanley, R. & Tiller, J. S. (Eds.) (2013). *Information Security Management Handbook,* Sixth Edition, Vol. 7. Boca Raton. CRC Press,Taylor and Fransic Group.

Olugbode, M., Richards, R. & Biss, T. (2007). The role of information technology in achieving the organisation's strategic development goals: A case study. *Information Systems*, 32(5), pp. 641-648.

Orgill G., G. Romney, M. Bailey and P. Orgill (2004), “The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems”, in *Proc. of the 5th Conference on Information Technology Education*, pp. 177-181.

Oxford (1952) Publications, The Advanced Learner's Dictionary of Current English.

Palmer, S. (2005), Can eBay be saved? *OnlineSPIN*. MediaPost Publications.

Patton, M. (1990), *Qualitative Evaluation and Research Methods*, 2nd edn, Newbury Park SAGE.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet research,* 14(3), pp. 224-235.

Ponemon Institute, (2011) *Cost of Data Breach Study: United States,* available at http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf (Accessed: 15 January 2015).

Prasad P. (2005), Crafting Qualitative *Research: Working in the Post-positivist Traditions*, New York. M.E. Sharpe

Raj, S. N. (2015). *Evaluation Of Cybercrime Growth And Its Challenges As Per Indian Scenario*.

Rajasekar, S and Philominathan, P (2013), *Research Methodolog*y, India, Physics.ed-ph.

Ramady M.A. (2014), *Political, Economic and Financial Country Risk: Analysis of the Gulf Cooperation Council*, Switzerland. Springer Science & Business Media.

Ratiu, C., Craciun., M.D. & Bucerzan, D. (2011). Statistical Model of The People Confidence In E-Business Services. *Analele Universitatii Maritime Constanta*, 51, (14) 237-240, available at: http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=59564746&site (Accessed: 4 January 2015).

Redman, L. V. & Mory, A. V. H. (1923). *The Romance of Research.* The Williams & Wilkins Company, Baltimore.

Reid, A. & Ryder, N. (2001). For whose eyes-only? A critique of the United Kingdom's Regulation of Investigatory Powers Act 2000. *Information and Communications Technology*, 10 (2) pp.179–201.

Remenyi, D. and Williams, B. (1996), The nature of research: qualitative or quantitative, narrative or paradigmatic? *Information Systems Journal*, 6(2), pp.131–146.

Rho, J. J. (2007), Blackbeards of the twenty-first century: Holding cybercriminals liable under the Alien tort statute. *Chicago Journal of International Law*, 7(2), pp. 695–719.

Ridley D. (2008), *The Literature Review: A Step-by-step Guide for Students* (First Edition), Sage Publications Ltd., London.

Riessman, C. K. (1993). *Narrative Analysis,* Sage Publications, Newbury Park, CA.

Rizzardi, R. (2008). Financial Management -- Payment Card Fraud Can Happen to You. *Optometry & Vision Development*, 39, (2) pp.64-65.

Roberds, W. (1998). The impact of fraud on new methods of retail payment. *Economic Review*, (1), pp. 42-52.

Rule, C. (2003). *Online dispute resolution for business: B2B, ecommerce, consumer, employment, insurance, and other commercial conflicts*, CA, John Wiley & Sons.

Rutter, J. (2000), '*From the Sociology of Trust Towards a Sociology "E-Trust*"' available at: http://les1.man.ac.uk/cric/Jason_Rutter/papers/eTrust.pdf.(accessed: 12 February 2015).

Sait, SM, Al-Tawil, KM & Hussain, SA (2004), 'E-commerce in Saudi Arabia: Adoption and Perspectives', *Australasian Journal of Information Systems,* vol. 12, no. 1, pp. 54-74.

Samba Bank, available at: http://www.samba.com/en/personal-banking/ways-to-bank/samba-access.html (Accessed: 14 March ,2015).

Sampson, R. J., Morenoff, J. D., and Gannon-Rowley, T. (2002) "Assessing 'Neighborhood Effects': Social Processes and New Directions for Research," *Annual Review of Sociology* (28), pp. 443-478.

Sandywell, Barry. (2010): "On the globalisation of crime: the Internet and new criminality." *Handbook of Internet crime*, pp. 38-66.

Sarantakos, S. (2005), Social Research, *Education,* 3rd ed. Macmillan Melbourne.

SAS Institute (1996), *Using Data Mining Techniques for Fraud Detection: A Best Practices Appoach to Government Technology Solutions.* Whitepapers. Available at http: iiwww.sas.com (Accessed: 22 November 2014).

Sathye, M. (1999). Adoption of Internet banking by Australian consumers: an empirical investigation. *International Journal of Bank Marketing*, 17(7), pp. 324-334.

Saudi Arabia Filter site (2009) available at: https://opennet.net/sites/opennet.net/files/ONI_SaudiArabia_2009.pdf (Accessed: 1 February 2015).

Saudi Arabia online users (2014) available at: http://www.internetworldstats.com/middle.htm (Accessed: 13 March 2015).

Saudi Ministry of Commerce (2001), *E-commerce in the kingdom: Breakthrough for the future, Riyadh*. Saudi Ministry of Commerce.

Schiffbauer, M., Sahnoun, H. & Keefer, P. (2014). *Jobs or Privileges: Unleashing the Employment Potential of the Middle East and North Africa*. World Bank Publications, Washington DC.

Shavers, B. (2013). *Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects*. 1st edition UK. Syngress.

Shah, M. H. (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce,* 18(2).

Singer P.W. & Friedman A. (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*. USA, Oxford University Press

Smith, J. A. & Osborn, M. (2003), Interpretative phenomenological analysis. In J. A. Smith (Ed.), *Qualitative Psychology: A Practical Guide to Methods*. London: Sage.

Sidden, K. & Simmons, D. (2005). Banking on security. American City & County, 120, (11) 30.

Snyder, J.M. (2000), Online auction fraud: Are the auction houses doing all they should or could to stop online fraud? *Federal Communications Law Journal* 52, 2, pp. 453–472.

Spann D.D. (2013), *Fraud Analytics: Strategies and Methods for Detection and Prevention*, 1 edition. Hoboken, New Jersey, Wiley.

Stajano, F. & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. *Communications of the ACM*, 54(3), pp. 70-75.

Stamler R.T., Marschdorf H.J. and Possamai M. (2014), *Fraud Prevention and Detection: Warning Signs and the Red Flag System*, 1 edition. Boco Raton .FL. CRC Press.

Stebbins, Robert A. (Ed.) (2001) *Exploratory research in the social sciences (Vol. 48)*, Sage, Thousand Oaks. CA.

Straub, D. W. and Welke, R. J. (1998), Coping with systems risk: Security planning models for management decision making", *Management Information Systems Quarterly*, 22(4), 441.

Straub, D. W. and Welke, R. J., (1998), "Coping with Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly*, pp. 441-469.

Strauss, A. & Corbin, J. (1998), *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Thousand Oaks, CA: Sage.

Stavroulakis P. & Stamp M. (2010), *Handbook of Information and Communication Security*,Verlag, Springer.

Stringham, E. (2005). The Capability of Government in Providing Protection against Online Fraud: Are Classical Liberals Guilty of the Nirvana Fallacy. *Journal of Law, Economics and Policy*, Vol. 1, No. 2, pp. 372- 2005.

Taylor, R. B. (1996, March). Neighborhood responses to disorder and local attachments: The systemic model of attachment, social disorganization, and neighborhood use value. In *Sociological Forum* (Vol. 11, No. 1, pp. 41-74). Kluwer Academic Publishers-Plenum Publishers.

The internet economy in G-20 (2012), available at: https://www.bcg.com/documents/file100409.pdf (Accessed: 22 March, 2015).

Thompson S. & Thompson N. (2008), *The Critically Reflective Practitioner*, Palgrave Macmillan.

Tiller J.S. & O'Hanley R. (2013), *Information Security Management Handbook*, Auerbach Publications.

Triplett, R. A., Gainey, R. R. & Sun, I. Y. (2003). Institutional strength, social control and neighborhood crime rates. *Theoretical Criminology*, 7(4), 439-467.

Tryfos P. (1996), *Sampling Methods for Applied Research: Texts and Cases*, New Jersey. John Wiley & Sons.

United Nations (1997). *UN manual on the prevention and control of computer related crime.* New York: United Nations.

Urquhart C. (2012), *Grounded Theory for Qualitative Research: A Practical Guide*, Sage Publications Ltd London.

U.S. Department of Commerce (2011), *Doing Business In Saudi Arabia: A Country Commercial Guide for U.S. Companies*, U.S. & Foreign Commercial

Service and U.S. Department of State. Available at: http://www.wtri.org/CCGSaudiArabia2011.pdf (Accessed: 22 March, 2015).

Vacca, J. R. (2007). *Biometric technologies and verification systems*. Oxford. Butterworth-Heinemann.

Van Maanen, J. (1998). Different strokes: Qualitative research in the Administrative Science Quarterly from 1956 to 1996. *Qualitative studies of organizations*: 8-33. Thousand Oaks, CA: Sage.

Vandommele, Tjark. *"Biometric authentication today"*.

Wall D.S. and Williams M. (2014), *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*, 1 edition, New York, Routledge.

Walsham, G. (ed) (1993), *Interpreting information systems in organisations*, New York, Wiley and Sons.

Warren W.D. and Walt S.D. (2007), *Payments and Credits*, 7th edition, Budapest Foundation Press.

Waters, R. (2003), How fraudsters set traps and take the credit. *Financial Times* IT.

Weber S. (2011), eBay 101: *Selling on eBay For Part-time or Full-time Income*, US. Weber Books.

Wells, J. T. (Ed.). (2009). *Computer fraud casebook: the bytes that bite.* Hoboken, New Jersey, John Wiley & Sons.

Weston, L. (2009). *Your Credit Score, Your Money & What's at Stake* [Updated Edition]: *How to improve the 3-Digit Number that Shapes Your Financial Future*. New Jersey. FT Press.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24(1), pp. 43-57.

Wilhelm, W. K. (2004). The fraud management lifecycle theory: A holistic approach to fraud management. *Journal of economic crime management*, *2*(2), 1-38.

Willig, C. (2003), Discourse analysis. In J. A. Smith (Ed.), *Qualitative psychology: A practical guide to research methods*, pp. 159-183, London: Sage.

Wired News (2003) *Read this before buying on eBay* [Reuters]) available at: www.wired.com/news/ebiz/1,57153-0.html (Accessed at 15 December 2014).

Women 4 times more likely than men to give passwords for chocolate" (2008), *Infosecurity Europe*, Available at: http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1071 (Accessed: 23 November 2015).

Xiao, B. & Benbasat, I. (2011). Product-related deception in e-commerce: a theoretical perspective. *MIS Quarterly*, 35(1), pp.169-196.

Yar, M. (2008) "The Internet and Human Security" in R. Munck & G. Honor-Fagan eds, *Globalisation and Human Security: An Encyclopaedia*, 2 Volumes. Praeger Press.

Yar M., (2006), *Cybercrime and society*, Sage Publications Ltd., London.

Yin, R. K. (2003), Case study research design and methods. *Applied social research methods*, third edition, series 5.

Appendix B

The Impact of Countermeasures in the Control and Prevention of Online Fraud in Saudi Arabia and the Influence of the Environmental Context

Faisal Alanezi

Perception

1. **What do you consider to be online fraud?**

2. **How do you perceive online fraud – do you consider it a criminal activity?**

Awareness

1. **How would you describe your level of awareness of online fraud and how has it affected the combating of online fraud?**

2. **How often do you encounter online fraud**

Technological Measures

1. **Do you have technological, systems and procedural measures used to deter, prevent and detect online fraud?**

2. **What is the focus of these measures in place and how effective have they been?**

3. **Are these measures adequate enough?**

Regulations

1. **What sort of regulations do you have or rely on?**

2. **How do you view the government's regulations to deter, prevent, detect and penalise online fraud?**

3. **Do you see the regulations in place adequate?**

Enforcement

1. **How do you see online fraudsters prosecuted?**

2. **How prepared are the enforcement agencies both in government and other individual organisations?**